A Hogan Lovells White Paper

Pan-American Governmental Access to Data in the Cloud

A comparative analysis of seven Latin American jurisdictions to the United States

by

Christopher Wolf, Washington, DC
Bret Cohen, Washington, DC*

17 July 2014

Introduction

In a few short years, Cloud computing has become an indispensable information technology resource for business. The Cloud promotes efficiency and economy, and facilitates ready access to computing services and electronic data from anywhere in the world.

With increased business use of the Cloud to process and store data, however, concerns about government access to data in the hands of Cloud providers also has increased. When and how governments can access user data is not well-understood.

This White Paper examines the legal bases for governmental access to data in the Cloud in Latin America and compares them to laws regulating similar access in the United States. It builds on our previous Hogan Lovells White Paper on governmental access to Cloud data in certain European, Asian, and North American countries,[1] asking the same questions under the laws of Argentina, Brazil, Chile, Colombia, Mexico, Panama, and Peru. "Governmental access," as that term is used here, includes access by all types of law enforcement authorities and other governmental agencies, recognizing that the rules may be different for ordinary law enforcement and national security access.

An indisputable premise of this White Paper is that governments need some degree of access to data for criminal investigations and for purposes of national security. But the right of individuals to maintain the privacy of their communications and documents from unreasonable government intrusion also is an extremely important issue. This White Paper does not enter into the ongoing debate about the potential for excessive government access to data and sufficiency of current procedural protections. Rather, it aims to compare the nature and extent of governmental access to data in the Cloud in jurisdictions across the Americas.

Cloud Adoption Tempered by Misconceptions

Latin American Cloud adoption and growth is expected to increase dramatically over the next few years.[2] This growth has been accompanied by concerns about where and how that information is stored, particularly when hosted in a foreign country. For example, with respect to data stored with U.S.-based Cloud service providers, there is a commonly-expressed belief that the **2001 USA PATRIOT Act** ("Patriot Act") gives the United States government greater powers of access to personal data in the Cloud than governments elsewhere. However, as we explain in this White Paper, Latin American jurisdictions grant similar rights of access to Cloud data. Unfortunately, there are misconceptions about what the law allows, at home and abroad, which creates false assumptions about Cloud services.

Such misconceptions encourage speculation that governmental access to data stored in the Cloud is more likely in some places than in others, and that the best way to limit such access is to use Cloud service providers present only in "safe" jurisdictions – places where data are thought to be free from problematic governmental access. The assumption that by choosing a Cloud service provider based on its location, data stored in the Cloud will be more secure and less subject to governmental access often is not supported by the facts.

* Special thanks to Hogan Lovells colleague Julian Flamant for his assistance in preparing this White Paper, and to Pablo Palazzi (Argentina), Leonardo Palhares (Brazil), Caio Iadocico de Faria Lima (Brazil), Paulina Silva (Chile), Andrés Felipe Umaña (Colombia), Irene Velandia Rodríguez (Colombia), Jorge Léon-Orantes (Mexico), Paola Morales (Mexico), Carlos González (Panama), and Juan José Cárdenas (Peru) for their assistance in the study of the laws in their respective countries.

[1] Winston Maxwell & Christopher Wolf, *A Global Reality: Governmental Access to Data in the Cloud* (2012), *available at* http://hldataprotection.com/2012/05/articles/international-eu-privacy/hogan-lovells-white-paper-on-governmental-access-to-data-in-the-cloud-debunks-faulty-assumption-that-us-access-is-unique.

[2] *See* Cisco Global Cloud Index: Forecast and Methodology, 2012-2017, at 25 (2013), *available at* a http://cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.pdf.

Summary of Conclusions

On the fundamental question of governmental access to data in the Cloud, we conclude, based on the research underlying this White Paper, that the physical location of Cloud servers does not significantly affect government access to data stored on those servers. Governments across Latin America retain broad rights to retain and access data stored by private companies in the Coud. Fundamentally, it is incorrect to assume that the United States government's access to data in the Cloud is greater than that in the Latin American jurisdictions that we examined.

In addition to domestic legal frameworks enabling governmental access to data within a country, **Mutual Legal Assistance Treaties ("MLATs")** and other foreign treaties, which are in effect between and among countries around the world, can provide governments the ability to access data stored in one jurisdiction but needed for lawful investigative purposes in another. Despite the procedural hurdles that may exist to request and obtain information pursuant to MLATs, these treaties make borders and the physical location of data much less significant barriers to governmental access.

On a related issue, there is significant discussion today about the power of a government to require a party in its jurisdiction to access and produce data stored in *another* jurisdiction, based on principles of physical presence of the party (not the data, or where the party is headquartered). In other words, the fact that a business located in one country may have chosen to store its data in the Cloud in another country does not mean that the business is immune from governmental demands for the production of that off-shored data.

Notably, our examination of governmental authorities' ability to access data stored in or transmitted through the Cloud revealed that **every single country that we examined vests authority in the government to require a Cloud service provider to disclose customer data and to intercept data transmitted to or from the servers of Cloud service providers.** Moreover, the laws of only a minority of the countries surveyed purported to preclude law enforcement access to foreign servers. And despite those laws, one commentator has noted, based on discussions with Latin American law enforcement experts, that in practice if a search warrant grants access to a location and, in turn, to the computer terminals there, law enforcement officers will access data from a terminal regardless of where the data are held.[3] Finally, MLATs and other foreign treaties can be used to allow access to data across borders.

Furthermore, as we describe in this White Paper and as illustrated in the chart at the end, in all of the Latin American jurisdictions surveyed except Chile and Panama, and in most cases Brazil, there is the real potential of data relating to a business or person, but not technically "personal data," stored in the Cloud being disclosed to governmental authorities *voluntarily*, without legal process and protections. In other words, governmental authorities can use their "influence" with Cloud service providers – who, it can be assumed, will be incentivized to cooperate since it is a governmental authority asking – to hand over information outside of any legal framework. One account goes so far as to describe that in practice, many Latin American Cloud service providers enter into informal agreements with law enforcement authorities that detail what information it will provide to the authorities and under what circumstances, outside of the scope of judicial review.[4]

United States law specifically protects *any type* of Cloud customer data to the government without a formal legal request, unless certain limited exceptions apply, such as in the event of an emergency involving death or serious bodily injury requiring disclosure. Cloud providers in the U.S. face civil and criminal penalties for violating the laws against voluntary disclosure to the government.

Furthermore, in situations where a Cloud service provider is compelled to supply customer data to the U.S. government, the customer must be notified except where the government takes the step of applying for a search warrant, or where the government certifies that disclosure would compromise the investigation (in which case notification may be delayed). U.S. courts have applied this rule equally to non-U.S. citizens who store their data with U.S. Cloud service providers. None of the Latin American countries that we surveyed required notification to customers, except in Mexico where the disclosure to law enforcement is of personal data being processed on behalf of another organization.

In addition, Colombia does not require prior judicial authorization in a number of law enforcement scenarios, including when the government seeks to search Cloud databases for proprietary (but non-personal) information and when a prosecutor seeks to intercept communications or transfers taking place over a communications network. These scenarios both require prior judicial authorization in the United States.

[3] Marcos Salt, *Transborder Access to Stored Computer Data in Latin American Countries*, at 4-5 (2012), *available at* http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_octopus2012/presentations/Octopus_2012_MarcosSalt_transborder_in_Latam.pdf.

[4] *Id.* at 5.

We conclude that civil rights and privacy protections related to governmental access to data in the Cloud are not significantly stronger or weaker in any one jurisdiction, and that any perceived locational advantage of stored Cloud data can be rendered irrelevant by MLATs and other foreign treaties. Our review reveals that businesses mislead themselves and their customers if they rely on an assumption that selecting Cloud service providers based in one jurisdiction or another better insulates data from governmental access. Instead, our study indicates that it is in business' interest to support governmental cooperation in this area, as it is the consistent and reasonably restrained exercise of existing legal authorities that will enable the economic growth and other benefits of Cloud computing.

Methodology

As with our previous White Paper, to conduct our examination, we consulted with experienced local counsel knowledgeable about data protection and governmental access law in each of the jurisdictions on which we report, asking the following questions for each jurisdiction:

1. May government require a Cloud provider to disclose customer data in the course of a government investigation?
2. May a Cloud provider voluntarily disclose customer data to the government in response to an informal request?
3. If a Cloud provider must disclose customer data to the government, must the customer be notified?
4. May government monitor electronic communications sent through the systems of a Cloud provider?
5. Are government orders to disclose customer data subject to review by a judge?
6. If a Cloud provider stores data on servers in another country, can the government require the Cloud provider to access and disclose it?

We start with an overall review of MLATs. These treaties effectively make a country's borders less significant for purposes of governmental access to data, and likewise make less significant the location of a Cloud service provider within one country's borders as opposed to another country's borders. We then review the situation with respect to governmental access in the United States and proceed to examine the situations in Argentina, Brazil, Chile, Colombia, Mexico, Panama, and Peru.

1. MUTUAL LEGAL ASSISTANCE TREATIES

Governmental authorities are able to reach data stored on the servers of a Cloud service provider over whom they do not have jurisdiction through an **MLAT** with a foreign nation where the Cloud service provider is based. For example, the United States has entered into bilateral MLATs with a number of Latin American countries, including Brazil, Mexico, Panama, Uruguay, and Venezuela, which allow governmental authorities in each country to request access to data stored on the servers of a Cloud service provider physically located in or subject to the jurisdiction of the foreign nation. Other treaties between the United States and Latin American countries allow for mutual assistance in criminal investigations. For example, the United States and seventeen other Latin American countries are signatories to the Inter-American Convention on Letters Rogatory, which enable the transmission of formal requests from courts in either country for judicial assistance.

The existence of these treaty relationships diminishes any perceived advantage of placing data with a Cloud service provider in a jurisdiction believed to permit less governmental access than other jurisdictions covered by the treaties. For all practical purposes, the laws permitting governmental access by the requesting country have their reach extended through operation of the treaties. For this reason, proposed laws that would require foreign companies to store all local data in-country would not shield data from foreign government access where such treaties are in place.

2. UNITED STATES

Any discussion of U.S. government access to data in the Cloud needs to begin with the Patriot Act, which commonly, but erroneously, is believed to have created invasive new mechanisms for the United States government to get information. The reality is that most of the investigatory methods in the Patriot Act were available long before it was enacted. And those investigative tools had, and still have, limitations imposed by the United States Constitution and by statute. It is more accurate to say that the Patriot Act did not create broad new investigatory powers but, rather, expanded existing investigative methods, **and retained Constitutional and statutory checks on abuse.**

Even with the Patriot Act, it is generally the case in the United States that the more substantive the data sought by the government, the greater the government's burden of demonstrating a strong legal justification to obtain that data. That is, there are greater restrictions on accessing the contents of electronic files and communications ("content data") than for other information associated with those files such as the file owner's contact information and server log information ("non-content data").

In most circumstances, governmental access to data stored by a Cloud service provider is regulated under the Electronic Communications Privacy Act ("ECPA"). Under ECPA, if a government body seeks disclosure of customer

data from a Cloud service provider, it can only do so if a legal mechanism is used – if a judge issues a **search warrant** or special **ECPA court order**, or if the government issues a valid **subpoena** to the provider. The legal mechanism to be used depends on the category of information:

- A search warrant issued upon a finding of **probable cause** that a crime has been committed is required under ECPA when the government seeks email that is stored in the Cloud for 180 days or less, whereas an ECPA court order or subpoena can be used to request stored email more than 180 days old, or any documents or data stored in the Cloud.[5]

- A judge can issue an ECPA court order for Cloud data only if the government demonstrates that there exist **reasonable grounds to believe** that the data sought are relevant and material to an ongoing investigation.

- Prosecutors and other government investigators may issue subpoenas requesting Cloud data directly to Cloud service providers if the data are **relevant to the investigation**.

If the government requests customer content data from a Cloud service provider through an ECPA court order or a subpoena, the government must notify the customer before obtaining the requested data from the provider unless it can demonstrate that providing prior notice would result in danger to a person's physical safety or compromise the investigation, in which case notice may be delayed. Where such delay is not sought by the government, the customer can challenge the governmental request. However, no prior notice is required to customers when the government requests (i) non-content data or (ii) content data via a search warrant, although customers can challenge the validity of search warrants in court after the data are produced.

Significantly, ECPA prohibits Cloud service providers from **voluntarily** disclosing customer data stored on their servers to the government without having received a formal legal request, unless certain limited exceptions apply, such as a provider's good faith belief that an emergency involving danger of death or serious physical injury requires disclosure.

And ECPA prohibits the United States government from intercepting electronic data in transit unless a judge determines that there exists **probable cause** to believe that the data will contain evidence of a crime, and that normal investigative procedures (i) have been tried and failed, (ii) reasonably appear to be unlikely to succeed if tried, or (iii) are too dangerous. When the government cannot obtain the required evidence in time and there is an emergency situation involving a danger of death or serious physical injury, issues of national security, or organized crime, the government can intercept electronic data without a judicial order, but must apply for an order within forty-eight hours after the interception has occurred.

Outside of these customary methods of access to Cloud data under ECPA, the U.S. government can access Cloud data through **FISA Orders** and **National Security Letters ("NSLs")** during the course of certain counterterrorism or foreign intelligence investigations.

- A judge can issue a FISA Order authorizing the government to obtain **content data** if the government demonstrates that there exist **reasonable grounds to believe** that the data sought are relevant to an investigation to obtain foreign intelligence or to protect against international terrorism or spying.

- Government investigators may issue special administrative subpoenas called NSLs directly to Cloud service providers. NSLs request certain **non-content data** about their customers – specifically subscriber information, length of service, and certain transactional records – if the government certifies that the request is relevant to an investigation to protect against international terrorism or spying. **The United States government may not use NSLs to obtain access to the *content* of electronic records and documents stored on a Cloud service provider's servers.**

FISA Orders and NSLs were available to the United States government even before the Patriot Act was enacted. The Patriot Act merely expanded some of the provisions of these access methods. For example, it added "gag order" provisions prohibiting recipients of FISA Orders or NSLs from disclosing the fact that they have received an NSL, except as necessary to comply with or challenge the request, and expanded the types of information obtainable through FISA Orders. A federal court recently held these gag orders unconstitutional in the context of NSLs, so depending on the outcome of appeals

[5] An influential U.S. appeals court has held that a search warrant is always required to access the contents of email stored in the Cloud pursuant to a search warrant, regardless of the number of days the emails have been stored with the Cloud provider. *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). Notably, in recent debates regarding the amendment of ECPA, the U.S. Department of Justice has conceded that a search warrant should be required for all stored email, making it likely that the 180-day distinction will be eliminated from the next version of the law. *See* Center for Democracy & Technology, Analysis of Department of Justice March 19, 2013 ECPA Testimony at 1-2 (April 8, 2013), *available at* https://cdt.org/files/pdfs/Analysis%20of%20DOJ%20ECPA%20testimony.pdf.

in that case, those gag orders may no longer have legal effect.[6]

There are, however, meaningful limitations on United States government access to Cloud data through FISA Orders and NSLs. First and foremost, their use is limited to certain counterterrorism or foreign intelligence investigations, so the government cannot use these methods to obtain documents and records for the sole purpose of investigating domestic criminal activity. A Cloud service provider has the ability to oppose a FISA Order before the issuing court, and also can seek judicial review of an NSL, which can be set aside "if compliance would be unreasonable, oppressive, or otherwise unlawful." A Cloud service provider also may petition the court to overturn the "gag order." And even though FISA Orders can require a Cloud provider (or any other business) to produce "business records" (a term that would encompass Cloud data), the United States government rarely requests them. In 2012, the government only made 212 applications for FISA Orders granting access to business records.[7]

U.S. courts, like those in other countries, have ruled that the U.S. government can use its own legal mechanisms to request data from any Cloud server located anywhere around the world so long as the Cloud service provider is subject to U.S. jurisdiction: that is, when the entity is based in the United States, has a subsidiary or office in the United States, or otherwise conducts continuous and systematic business in the United States.

In sum, governmental authorities in the United States cannot access data stored in the Cloud at will. Rather, governmental authority is circumscribed by the United States Constitution and state constitutions, judicial oversight, and laws and procedures enacted through the democratic process. In addition, and relevant to the concerns of foreign countries about their nationals' data, a recent ruling by a United States appeals court one level below the Supreme Court confirmed that ECPA's statutory protections are extended to *non-United States citizens* for data physically maintained in the United States and stored in the Cloud.[8]

3. ARGENTINA

Argentine government officials can gain access to customer data from a Cloud service provider by obtaining a **court order** to present information, and can intercept electronic transmissions to and from a Cloud service provider through a **court order** for a wiretap. To obtain either court order, the government must demonstrate to a judge that it has reasonable grounds to believe that a crime was committed or an illicit act took place.

Cloud service providers can voluntarily disclose customer data in response to an informal government request unless that data includes personal information, which under data protection law only can be disclosed under limited circumstances, such as pursuant to a judicial order, with the consent of the data subject, or in certain emergency situations. Where permitted by law, Cloud service providers do not have an obligation to inform their customers prior to disclosing their data to the government.

The procedure through which Argentine government officials request access to data from a Cloud service provider in investigations involving terrorism or national security concerns is similar to other criminal cases. Argentina's intelligence law, which governs government investigations in these circumstances, expressly requires a court order to access data stored online or to intercept electronic transmissions.

Argentine government data access procedures do not empower government authorities or courts to compel local companies to disclose data that is held on servers in foreign jurisdictions. In practice, Argentine government officials rely on the assistance of foreign authorities and established MLATs to gain access to foreign servers.

4. BRAZIL

Brazilian law enables government authorities, including both law enforcement and administrative agencies, to require a Cloud service provider to disclose customer data using a **search and seizure warrant** or **direct disclosure order**. Upon petition from a competent government authority, a judge will consider a request for such a warrant or order and grant it if the judge determines that the request would serve to further an investigation of a violation of a law or legal right.

Under the Brazilian Communications Statute, law enforcement authorities also can seek an **interception order** authorizing the interception of electronic communications, including data traveling to and from a Cloud service provider. Interception orders are more closely regulated than search and seizure warrants or direct disclosure orders, requiring law enforcement to demonstrate to a judge that (i) there is a reasonable indication that the investigated person participated in a crime; (ii) the evidence cannot possibly be obtained by any other available means; and (iii) the crime under investigation is a felony punishable by detention.

---

[6] *In re Nat'l Sec. Letter*, 930 F. Supp. 2d 1064 (N.D. Cal. 2013).
[7] *See* Letter from Peter J. Kadzik, Principal Deputy Ass't Att'y Gen., U.S. Dep't of Justice, to The Hon. Harry Reid, Majority Leader, U.S. Senate (Apr. 30, 2013), *available at* http://fas.org/irp/agency/doj/fisa/2012rept.pdf.
[8] *Suzlon Energy Ltd. v. Microsoft Corp.*, 671 F.3d 726 (9th Cir. 2011).

If a Cloud service provider voluntarily discloses a customer's personal information to the government in response to an informal request, it risks violating the Brazilian Internet Civil Rights Act, which took effect in June 2014. Under that law, Cloud service providers generally are prohibited from disclosing customer records or communications to the government without a judicial order.

In addition, under the fundamental right to privacy in the Brazilian Federal Constitution, if a Cloud service provider voluntarily discloses a customer's personal information to the government in response to an informal request, the service provider may be liable for any damages caused to the data subject as a result of that disclosure. Most Cloud service providers avoid such claims, however, by including provisions in their form customer agreements authorizing disclosure to the government in the course of investigations.

Notwithstanding these limitations on voluntary disclosure, Cloud service providers in some circumstances may be compelled by law to provide customer information to the government even in the absence of a judicial order. For example, the Internet Civil Rights Act permits Cloud service providers to disclose certain categories of personal data to law enforcement and administrative agencies without a judicial order when the requesting agency otherwise is authorized by law (such as, in certain circumstances, a person's name, address, marital status, and qualifications). Additionally, some Brazilian criminal laws require service providers to report certain conduct upon knowledge of its existence on their systems (e.g., the transfer of child pornography or the sale of smuggled or stolen goods).

Cloud service providers have no general obligation to inform customers when their data are disclosed to the government. In fact, investigations by the police and Public Prosecutor usually take place in secrecy and the government also may request an order for secrecy during the course of its investigations that would prohibit the Cloud service provider from informing the targeted customer of the investigation.

Brazil has no specific law governing government access to data for reasons of national security or terrorism. However, as with the investigation of other severe crimes, national security or terrorism cases may increase a judge's likelihood to require data disclosure.

Where a Brazilian Cloud service provider stores data on a server located in a foreign country, and can access that server from Brazil, the government can compel the service provider to access that server and provide any customer data that is responsive to a judicial order. In addition, Brazilian investigators can access Cloud data located in foreign countries through MLATs and other international agreements.

5. CHILE

To obtain customer data stored with or to intercept electronic communications made through the systems of a Cloud service provider (e.g., emails sent by or to a person, internet traffic, documents, or other communications), Chilean government officials must obtain a **judicial order**, which a judge will issue "when for motivated reasons its utility for a formal and open criminal investigation is foreseeable." Without a judicial order, Cloud service providers are prohibited from voluntarily disclosing customer data to the government without authorization from the customer or other legal authority. When a judge orders the disclosure of customer data, there is no obligation to notify the customer.

In investigations involving national security, terrorism, organized crime, or drug trafficking, judicial authorization still is required to obtain data from a Cloud service provider, although special procedures may apply. For example, the National Intelligence Agency (ANI) can apply to an appeals judge for an order authorizing the ANI to obtain electronic data directly from a Cloud service provider without notifying the provider, prosecutors can determine that certain actions, records, and documents must be kept secret from the target of the investigation, and judges can issue orders in emergency situations by telephone, fax, or email.

Chilean law does not authorize government officials or courts to require a Cloud service provider to disclose customer data that are stored exclusively on servers in foreign jurisdictions, although the government is entitled to access copies or backups of such data that are stored locally in Chile. There is no definitive legal ruling, however, as to whether the government can demand that a Cloud service provider produce customer data pursuant to a judicial order if the data are stored on foreign servers that are remotely accessible from the service provider's offices in Chile. In these situations, a Cloud service provider could argue that access to the foreign server is beyond the scope of the judge's warrant and jurisdiction. Alternatively, Chilean government officials can rely on MLATs or other formal diplomatic requests to access such data.

6. COLOMBIA

The Colombian government primarily relies on four legal mechanisms to require Cloud service providers to disclose customer data during the course of an investigation, each of which must be supported by reasonable grounds to infer that the data sought will contain evidence of a crime or will be relevant to an administrative investigation.

- First, a prosecutor may issue an **order to recover information** that permits the police to seize computers, servers, or other data storage devices in order to analyze and retrieve information relevant to a criminal investigation. These orders do not require prior judicial authorization, but are subject to review by a judge after the fact.

- Second, a prosecutor may issue an **order to search and compare information stored in databases** that permits the police to search and compare information stored in databases maintained by private or public organizations, including those maintained by Cloud service providers. If the search is for non-publicly-available personal information, the prosecutor must obtain judicial authorization before the search can take place. Otherwise, no judicial authorization is necessary.

- Third, a prosecutor may issue an **interception order** to intercept communications or transfers of data taking place over any communications network, including those maintained by Cloud service providers. The initial interception order is not subject to judicial review before the interception takes place, unless the prosecutor wishes to extend the duration of the initial order, in which case the prosecutor must obtain prior judicial authorization. After performing the interception, the police must file a report with a judge describing how the interception occurred, and within twenty-four hours of the receipt of the police report, the judge must review the legality of the order. Also, within thirty-six hours of the interception the police must present the information collected to the judge in a preliminary and private hearing to determine if the interception was performed legally.

- Fourth, during the course of an investigation by a public or administrative authority, the authority can issue an **administrative order** requiring that individuals and companies under its authority provide data stored in the Cloud, provided that (i) there is a strong nexus between the data requested and the authority's legal functions, and (ii) if any personal data are requested, the authority must process the data in compliance with Colombian data protection law.

Cloud service providers may voluntarily disclose customer data in response to informal requests from the government unless the data to be disclosed are subject to a legal privilege or confidentiality requirement. Protected data includes personal data covered by Colombia's data protection law, data subject to a professional privilege (e.g., attorney-client, banking, or medical confidentiality), and data protected as a trade or industrial secret. Claims of privilege are considered on a case-by-case basis, and Cloud service providers are prohibited from disclosing privileged data unless they receive an administrative or judicial order or, in the event of personal data, the data subject's authorization. If a lawful order authorizes the disclosure of Cloud data to the government, there is no general requirement that a Cloud service provider must inform its customers prior to disclosure.

Colombian law permits its intelligence agencies to monitor telecommunications networks, including data or communications in transit to and from a Cloud service provider, without prior judicial authorization as long as such activity does not involve actually intercepting a private communication. Therefore, business records stored with a Cloud service provider that do not constitute communications can be monitored without a judicial order. When consulted, judges are more likely to grant prosecutors' requests for data in the course of an investigation involving national security or terrorism than for an investigation of an ordinary crime.

Where a Colombian Cloud service provider stores data on a server located in a foreign country, and can access that server from Colombia, the government will most likely compel the service provider to access that server and provide any customer data that is responsive to a judicial order. In addition, Colombian investigators can access Cloud data located in foreign countries through MLATs and other international agreements.

7. MEXICO

Mexican authorities may require a Cloud service provider to disclose customer data in the course of a government investigation. The legal mechanism used by the government will depend on the subject matter of the investigation and the law that applies to each specific case.

During an ongoing criminal investigation or tax investigation, a public prosecutor or the tax authority may obtain a **search warrant** from a competent judge to obtain data stored in the Cloud if there are grounds to believe that the data are related to the commission of a crime or the breach of a tax law. In addition, certain administrative agencies can require a Cloud service provider to provide customer data, through the issuance of a **written order**, to determine the provider's compliance with the laws under the agency's purview. Although administrative agencies typically only use these orders to request information from the investigated entity or person, in some cases third party information can be disclosed. These requests require the agency to issue a written statement indicating the legal provision and reason on which the request is based. The legality of such requests can be reviewed by the same authority that issued the request or by its superior authority, depending on the subject matter. When a Cloud service provider is required to disclose customer data to a

government authority, it has no general obligation to inform the customer, although if it is processing personal data on behalf of and at the direction of another organization, it is required to notify the other organization that a government authority requested the personal data.

Mexican law enforcement authorities can intercept communications, including those sent through the systems of a Cloud service provider, only after receipt of a **judicial authorization**. To obtain a judicial authorization, an authority must demonstrate that sufficient evidence likely exists to prove that the subject of the surveillance was responsible for committing a serious crime, and must submit (i) the legal provisions on which its request is based, (ii) the reasons why the interception is needed, (iii) the types of communications sought, (iv) the persons for whom and places where the requested communications would be intercepted, and (v) the period during which the communications would be intercepted. Such authorizations are not available in electoral, tax, commerce, civil, labor or administrative matters.

Cloud service providers may voluntarily disclose customer data to government officials except for certain categories of data that are legally protected. These categories include personal data, data obtained by a person rendering professional or technical services, and all non-public information transmitted through telecommunications networks and services. Where such information is protected, a Cloud service provider would need to obtain consent or a written order from the competent authority before disclosing the information to the government.

Mexico has no specific law governing governmental access to data for reasons of national security or terrorism. In practice, however, a judge would be more likely to grant a prosecutor's request for data in the course of such an investigation.

Where a Mexican Cloud service provider stores data on a server located in a foreign country, and can access that server from Mexico, the government can compel the service provider to access that server and provide any customer data that is responsive to a search warrant. In addition, Mexican investigators can access Cloud data located in foreign countries through MLATs and other international agreements.

8. PANAMA

Panamanian law enforcement authorities may require a Cloud service provider to disclose customer data in the course of open investigations through an order of **judicial inspection** if it can demonstrate to a judge that there is probable cause to believe that a crime has been committed. Similarly, authorities can apply for a **judicial authorization** to intercept electronic communications sent through the systems of a Cloud service provider supported by evidence of the commission of a crime. In addition, administrative authorities can compel the disclosure of information related to their administrative work, without having to resort to judicial procedures. In the case of lawful disclosures under these procedures, the Cloud service provider has no obligation to inform customers that their information has been disclosed to the government.

Otherwise, Panama's Law Regulating Electronic Documents expressly prohibits any "database manager," a term that includes Cloud service providers, from voluntarily disclosing data without obtaining the approval of a judge.

Government authorities are not empowered to obtain a judicial inspection requiring a Panamanian Cloud service provider to disclose data stored on servers located in foreign jurisdictions, even if those servers can be accessed from Panama. Additionally, the Law Regulating Electronic Documents establishes a special regime that, on its face, prohibits the Panamanian government from accessing data stored in databases managed by foreign entities under any circumstance, even if those databases are stored on servers located in Panama. This broad protection seems to be the result of ambiguous drafting, but the Supreme Court of Panama has not yet interpreted it, so lower Panamanian courts may interpret the prohibition as broadly as its language suggests. Courts may be more likely to grant a judicial inspection of foreign-owned servers in serious criminal cases (e.g., related to terrorism, national security, or drug trafficking), but in such cases, a foreign database owner would have a good argument that the inspection violated the law. Notwithstanding these restrictions, Panamanian authorities can rely on MLATs and other treaties to request foreign governments to assist in accessing customer data stored on Cloud servers managed by foreign organizations, both domestic and abroad.

9. PERU

As a general rule, Peruvian government officials, within the scope of their powers and subject to due process guarantees, can require a Cloud service provider to disclose customer data in the course of any investigation. In criminal investigations, government investigators can request a **judicial order** to require a Cloud service provider to disclose customer documents or intercept customer communications if related to the objectives of the investigation and the disclosure does not violate a person's constitutional rights to the privacy of communications, personal and family intimacy, or the privacy of banking or tax information. In addition, administrative agencies may request information from a Cloud service provider necessary for investigations under each agency's jurisdictional authority, typically in the form of an

administrative subpoena or **administrative warrant**, subject to judicial review and the same constitutional limitations as judicial orders.

It is lawful for Cloud service providers to voluntarily disclose data to government entities, except where such disclosures would infringe any of the constitutional protections mentioned above or would include personal data that would affect an individual's privacy without the informed consent of that individual. Private parties that disclose personal information from computerized databases in violation of these restrictions are subject to criminal penalties. Generally, Cloud service providers are under no legal requirement to notify their customers before lawfully disclosing customer data to the government, whether under criminal or administrative procedures.

In investigations into national security, terrorism, or drug trafficking, Cloud service providers (along with other organizations) are required to provide data upon request to the Peruvian National Intelligence System (SINA), unless the provision of such data would violate professional confidentiality obligations or an individual's previously mentioned constitutional right to privacy. SINA is obligated to keep this information confidential, so disclosure to SINA does not violate any right of confidentiality. In addition, SINA is permitted to request information from Cloud service providers and others strictly for intelligence purposes if it obtains a judicial order issued by two judges of the Supreme Court of Peru.

There are no legal restrictions that limit the government's ability to require a Peruvian Cloud service provider to retrieve data stored on servers in foreign jurisdictions. In addition, the criminal code includes procedures to facilitate international judicial cooperation to assist with the functioning of MLATs and other international requests for mutual assistance.

GOVERNMENTAL AUTHORITIES' ACCESS TO DATA IN THE CLOUD: A COMPARISON

	May government require a Cloud provider to disclose customer data in the course of a government investigation?	May a Cloud provider voluntarily disclose customer data to the government in response to an informal request?	If a Cloud provider must disclose customer data to the government, must the customer be notified?	May government monitor electronic communications sent through the systems of a Cloud provider?	Are government orders to disclose customer data subject to review by a judge?*	If a Cloud provider stores data on servers in another country, can the government require the Cloud provider to access and disclose the data?
Argentina	Yes	Yes, except for personal data without a legal purpose	No	Yes	Yes	No, not without cooperation of the other country's government
Brazil	Yes	Yes, except only when expressly authorized by law, and may be liable for damages caused by a disclosure of personal information where such disclosure is not anticipated in customer agreements	No	Yes	Yes	Yes
Chile	Yes	No – must request data through legal process	No	Yes	Yes	In principle, not without the cooperation of the other country's government, although there is no definitive legal ruling as to whether the government can demand production of data stored on foreign servers, and the government can require disclosure of any local copies
Colombia	Yes	Yes, except for personal data without a legal purpose	No	Yes	No, except for orders to intercept electronic communications that need to be extended; the seizure of computing equipment; and orders to search databases that contain personal information	Most likely yes
Mexico	Yes	Yes, except for personal data without a legal purpose, trade secrets, data subject to a professional privilege, and electronic communications	No, except for disclosures of personal data processed on behalf of and at the direction of another organization	Yes	Yes	Yes

* "Review by a judge" encompasses either an initial review when issuing the court order, warrant, etc. or subsequent review when the court order, warrant, etc. is challenged by the service provider or customer.

Panama	Yes, except ostensibly for databases managed by foreign organizations	No – must request data through legal process	No	Yes	Yes	No, not without the cooperation of the other country's government
Peru	Yes	Yes, except for personal data without a legal purpose, electronic communications, data affecting personal or family intimacy, and banking or tax information	No	Yes	Yes	Yes
United States	Yes	No – must request data through legal process	Yes, for content data, except when the government obtains a search warrant or unless disclosure would compromise the investigation	Yes	Yes	Yes