Forecasting the Impact of the New US CLOUD Act

Dechert LLP

Executive Summary

- The CLOUD Act resolves the central issue in *United States v. Microsoft* — **U.S. law enforcement agencies now have explicit legal authority to obtain electronic data from U.S. cloud and communication companies regardless of where the company stores the data**.
- The Act includes provisions that allow U.S. cloud companies to challenge such efforts when their customer is not a U.S. citizen or resident and the disclosure would violate the law of "qualifying" countries, **but the availability and efficacy of these protections are uncertain**.
- The CLOUD Act also proposes a legal framework for expeditious international data-sharing using executive agreements and an elaborate certification process by which countries can become **"qualifying foreign governments"** (QFGs). Countries that do pursue and obtain QFG status will provide greater privacy protection for their citizens and residents when their information is sought by U.S. law enforcement and will be **entitled to obtain electronic data from U.S. tech companies without prior approval or oversight of the U.S. government.**
- But **it is not clear if other countries will be interested in pursuing QFG status**. This is particularly true for the EU and its member states because **the CLOUD Act may conflict with the soon-to-be effective GDPR**. If so any executive agreement between the U.S. and the EU or an EU member state would require an act of the EU legislature.
- Given the growing volume of business and personal data stored in the cloud, the lack of any congressional legislative history, and the significant uncertainties arising from the structure and terms of the CLOUD Act, **cloud companies and their customers should continue to closely monitor these developments in this area. Other practical guidance steps are provided at the end of our analysis**.

CLOUD Act: Clarifying Lawful Overseas Use of Data

On March 23, 2018, President Donald J. Trump signed a US$1.3 trillion appropriations bill passed by Congress in a last-minute effort to avoid a federal government shutdown. The news storm surrounding the bill's passage largely obscured the fact that the 2,232-page spending measure included a bill called the "Clarifying Lawful Overseas Use of Data" or CLOUD Act.[1] Passage of the CLOUD Act resolved the issue currently before the U.S. Supreme Court in *U.S. v. Microsoft* — the Stored Communications Act now explicitly applies to data held by U.S. communications and cloud providers regardless of location.[2] Other provisions of the CLOUD Act, however, may significantly alter how non-U.S. law enforcement officials seek and obtain electronic communications and data in the hands of U.S. cloud service providers.[3] Given the accelerating trend to move business and personal data to cloud storage and the current dominance of U.S. companies in the cloud market, it is essential that companies understand the scope and impact of the CLOUD Act and monitor how it is implemented and interpreted, including how a number of key questions left unanswered by the legislation are resolved in the future.

The CLOUD Act makes four major changes to U.S. law:

- U.S. law enforcement agencies (both federal and state) now have express legal authority to seek electronic data in the possession, custody or control of U.S. electronic communications and cloud companies regardless of where the data is physically stored.
- U.S. cloud providers (not the owners of the data) can seek to quash or modify a request for data of a non-U.S. person when the disclosure would violate the laws of a "qualifying foreign government."
- The Act proposes a legal framework — subject to congressional disapproval but not judicial oversight — by which data-sharing executive agreements can be entered into with foreign governments certified by the U.S. Attorney General as having similar legal protections as the United States with respect to civil liberties, judicial process, data privacy and cybersecurity.
- Countries certified by the Attorney General (and not overturned by Joint Resolution of Congress) can seek disclosure of data held by U.S. cloud companies in the United States for criminal investigations without U.S. oversight or cooperation.

Significantly, **the CLOUD Act does not define the "cloud" or "cloud services."** Rather, it relies on existing definitions from the 1986 Electronic Communications Privacy Act. The new rules apply to providers to the public of "electronic communications services" or "remote computing" services (including both storage and processing services). *See* 18 U.S.C. §§ 2510(12), 2711(2). These definitions are quite broad and have been interpreted by U.S. courts to apply to U.S. companies providing e-mail, instant messaging, videoconferencing, wireless calling, remote or backup data storage, and cloud hosting or processing. (For ease of reference in this analysis, we will refer collectively to these U.S. companies as cloud service providers or CSPs). Thus, the CLOUD Act has potentially enormous implications for these companies and those that rely on their services.

[1] A copy of the CLOUD Act is available here. Companion versions of the bill were introduced on February 6, 2018 by Senator Orrin Hatch and Representative Doug Collins with bipartisan support. Both bills were referred to the respective Judiciary Committees of the U.S. Senate and House of Representatives. No committee took any formal action with respect to the CLOUD Act in the form of hearings, reports, or votes and there was no debate on the bill before it was passed.

[2] Indeed, just days after the CLOUD Act was passed the DOJ abandoned its original warrant and served a new warrant for the same data. The DOJ asked the Supreme Court to vacate and remand the case for dismissal because it was now moot, and Microsoft agreed, though the Court has not yet issued a ruling.

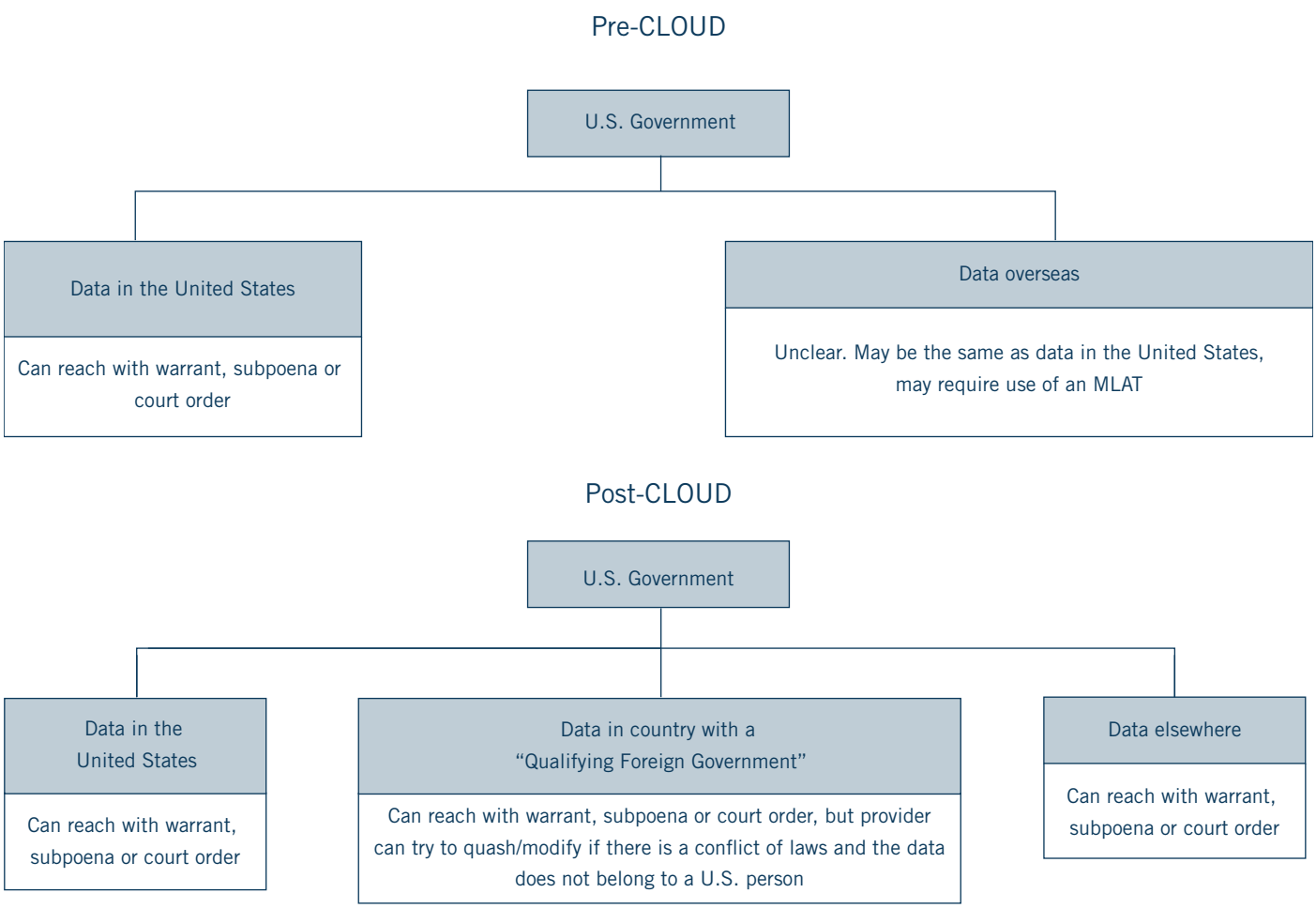
[3] Reaction to the Act's passage has been mixed. Technology companies have, for years, pushed for legislation to protect user privacy while supporting law enforcement in multi-jurisdiction investigations. In a recent blog post, Microsoft's President Brad Smith said the Act "is an important step forward, but now more steps need to follow." Privacy and civil liberties advocacy organizations continue to worry that the Act gives the U.S. government enhanced authorization to access data all over the world and could permit foreign governments to monitor and collect data on U.S. soil without any U.S. government oversight. Twenty-four groups, including the ACLU and the Electronic Frontier Foundation, signed a letter to Congress opposing the Act.

Location, Location, Location No Longer the Rule

Under the Stored Communications Act ("SCA"), U.S. law enforcement agencies can seek customer or subscriber information from CSPs, including the content of electronic communications. Legal limits are imposed on such requests depending on the data being sought and the type of legal process employed — warrant, subpoena or order from federal or state court. 18 U.S.C. § 2703. In many situations, the U.S. government must notify the subscriber or customer. Where notice might have adverse consequences, courts can temporarily delay notice and prohibit the service provider from telling the customer or subscriber about the government's request. 18 U.S.C. § 2705. CSPs can challenge the legality of a subpoena, and the government can move to enforce these orders through contempt proceedings as occurred in *United States v. Microsoft*.

In *Microsoft*, the U.S. Department of Justice (DOJ) served a criminal warrant on Microsoft for account information and e-mails as part of a criminal investigation. Microsoft provided the user's account information stored on servers in the United States but refused to turn over the e-mails themselves because they were stored on a server in the Republic of Ireland. Microsoft's position was that § 2703 only applied to data physically located within the United States absent language that

What Data Can the U.S. Government Reach?



Congress intended the SCA to apply outside the United States, and that a contrary reading would lead to "international discord." The DOJ argued that regardless of where the data was stored, the conduct at issue was domestic: a disclosure by a U.S. company to the U.S. government in the United States.

Section 3 of the CLOUD Act now expressly resolves the question before the U.S. Supreme Court in *Microsoft* by making clear that CSPs are obligated "to preserve, backup, or disclose any contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber" within the CSPs' "possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States." Thus, the CLOUD Act grants federal and state law enforcement officials explicit authority to issue subpoenas or seek warrants and court orders forcing CSPs subject to U.S. jurisdiction to preserve and produce data wherever the CSPs decide to store it on a global basis.

Motions to Quash or Limit Legal Process Filed by CSPs: Real or Illusory Protection?

To alleviate the potential for "international discord," the CLOUD Act also creates a new legal framework by which CSPs — not the account owner or subscriber — can challenge subpoenas or warrants served on CSPs that conflict with the laws of a "qualifying foreign government" (QFG) and do not involve U.S. persons or residents. The open question is how this framework will operate, and especially whether it will offer any protection before the executive agreements necessary for countries to qualify as QFGs are signed and certified (as described in detail below).

The CLOUD Act specifically authorizes CSPs to file a motion to quash or limit a warrant or subpoena aimed at electronic communications or stored data, but such a motion must be based on a reasonable belief that (1) the customer or subscriber is not a U.S. citizen, resident or company incorporated in the United States and (2) that the required disclosure "would create a material risk" that the CSP would be violating the laws of a "**qualifying foreign government**." The court can then grant a motion to quash or modify "only if the court finds" that: (1) the customer or subscriber is not a U.S. citizen, resident or a company incorporated in the United States; (2) that the disclosure "would cause" the CSP to violate "the laws of a **qualifying foreign government**;" and (3) that the interests of justice under the totality of circumstances "dictate that the legal process should be modified." To assess this last element, the court is required to apply an eight-factor comity analysis that looks at the competing interests of the countries involved, the customer's residence and connections to the involved countries, the CSP's connections to the United States, and the availability of reasonable alternatives.

As highlighted in the flowchart below, there is a condition precedent to both filing and potentially prevailing on a motion to quash or limit — **the existence of a QFG**. Currently, no QFGs exist because none of the legal and procedures requirements (detailed below) have been completed by which countries can be certified as QFGs. Under a literal reading of the CLOUD Act, therefore, no motion to limit or quash can be filed or be granted for a CSP.[4]

[4] The language and structure of the CLOUD Act further complicates these issues because of the conjunctive definition of a "qualifying foreign government" as one that has executive agreement certified to meet statutory criteria AND laws applicable to CSPs that provide the CSPs with "substantive and procedural opportunities" to seek judicial review of legal process that conflicts with laws of other governments and permits the disclosure of that process to those governments. As such, while Congress expressly exempted the certification process from judicial review, the determination that a country is a QFG appears to require a judicial finding in each case that the other requirements are satisfied.

May a Court Issue a Motion to Modify or Quash Legal Process Seeking Data Stored Outside the United States?

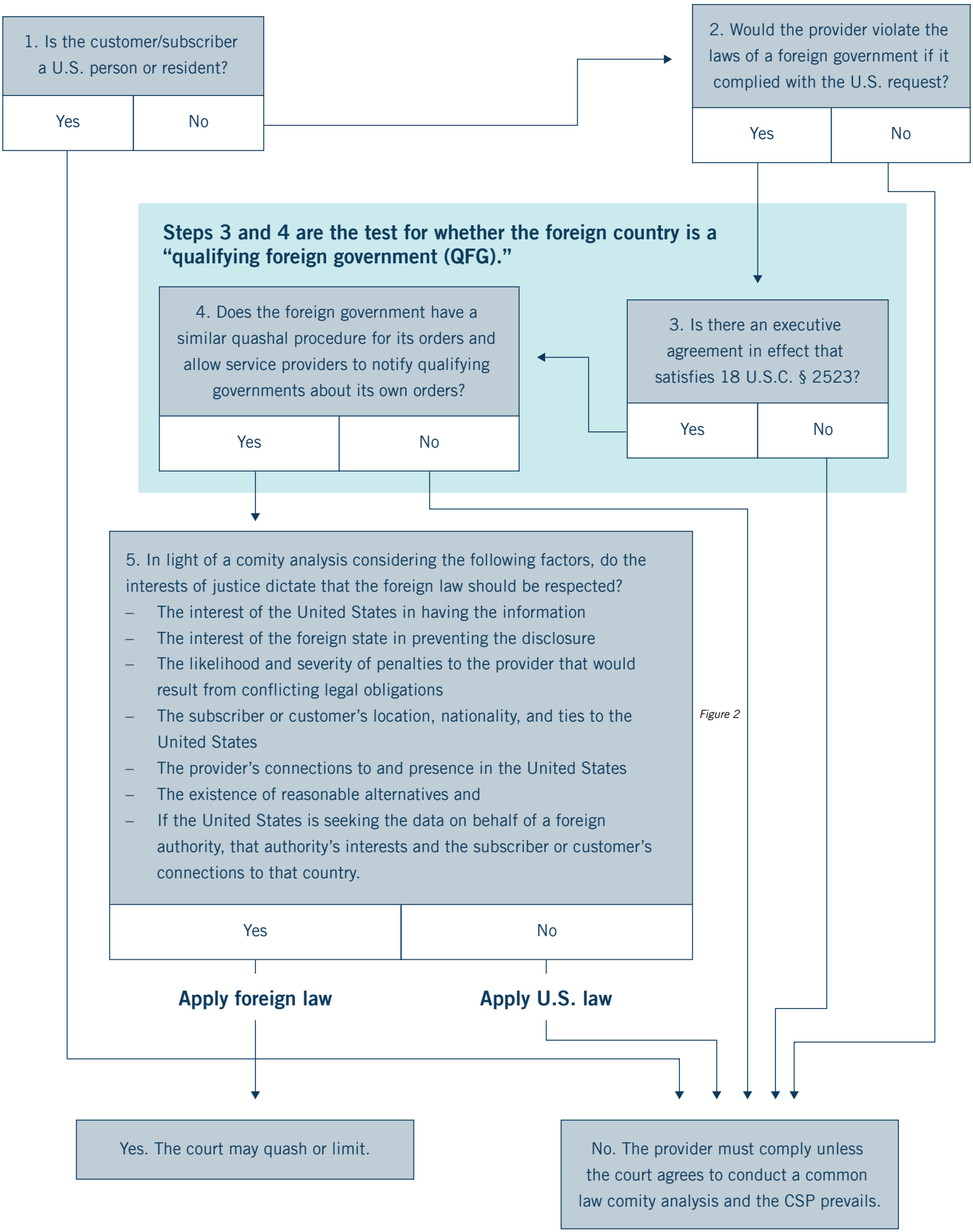


Figure 2

The availability of these motions practice protections will also depend on how many foreign countries are willing and able to accept the CLOUD Act's terms. For example, while many of the most likely candidates for QFG status are in Europe, the necessary agreements will be complicated by the EU's new General Data Protection Regulation (GDPR), which becomes effective in May 2018. It is unclear whether an agreement could satisfy both the CLOUD Act's requirements and GDPR, which heavily restricts data processing and production, especially when the data is sent outside the European Union (EU). If such agreements do not fit within an existing exception, an act of the EU legislature — comprising the EU Council and the EU Parliament — would be required to create a new exception to GDPR. That approval is unlikely given current European concerns about data privacy and alleged misconduct by the "Big Five" tech companies.[5] And on the U.S. side, it is unclear that the EU could ever be recognized as a QFG within the meaning of the statute because the requirements are stated in terms applicable to individual countries, not an economic union of multiple countries.

Additional uncertainty arises from the fact that, as detailed below, the certification process that is the to becoming a QFG is permissive, not mandatory. The U.S. Attorney General has the discretion to decide whether to begin the process by sending the written certification to Congress. If no certification is submitted to Congress, it would effectively bar the CSPs from filing or prevailing on any motion to quash or limit a warrant or subpoena. Since Congress expressly exempted the Attorney General's certification decision from judicial or administrative review, it will be difficult to articulate a legal basis to try to force the Attorney General to act in order to trigger the first step in the certification process on which the motion practice protections are based in the CLOUD Act.

Finally, it is also currently unclear how the DOJ will square the CLOUD Act with the December 2017 Policy Statement issued by the Criminal Division's Computer Crime and Intellectual Property Section which directed federal prosecutors, subject to some exceptions, to seek the electronic data directly from companies or enterprises that are the targets or subjects of investigations rather than from CSPs.[6]

Executive Agreements and QFG Status

The CLOUD Act established a new legal framework — based on conformity with U.S. law — that could support far greater and faster access to information and contents stored by U.S. CSPs. Countries that are determined to share U.S. legal policies and procedures, particularly with respect to individual rights and civil liberties, have "adequate" data privacy and cybercrime laws, and agree to a long list of terms can form bilateral executive agreements with the U.S. government that are "certified" by the Attorney General. Having a certified agreement is the main requirement for QFG status. Countries that cannot meet these requirements are ineligible for QFG status and will be at a comparative disadvantage when their privacy laws conflict with those of the United States. QFGs will be entitled to privileges over non-QFG countries in two areas.

First, the privacy laws of a QFG will be given more respect when CSPs receive legal process from U.S. law enforcement authorities aimed at citizens or residents of the QFG country. CSPs can disclose the existence of a U.S. subpoena or warrant to the foreign government even if there is a protective order generally barring disclosure. Finally, a conflict with a QFG's laws empowers the CSP to move to have an order modified or quashed if the customer being investigated is not a U.S. person or

[5] Facebook was recently fined US$122 million for misleading EU authorities over how it would use data acquired through its merger with WhatsApp and will probably face investigations over the Cambridge Analytica scandal. Microsoft was subject to a French investigation for allegedly collecting user data through Windows 10 until last year. Alphabet (Google) is currently before the European Court of Justice over the "right to be forgotten." Amazon and Apple have both been ordered to repay illegal tax breaks and have been involved in antitrust disputes with EU authorities. Approval might also be impacted by broader but related issues such as the ongoing work of the Article 29 Working Party on the EU-U.S. Privacy Shield.

[6] A copy of the CCIPS policy can be found here.

resident. Doing so will extend the potential privacy protections of the QFG to data being sought in the United States. As detailed above, this is not the case with non-QFGs, and CSPs may not be able to file or prevail on any protective motion absent convincing a court to engage in a common law comity analysis.

Second, QFGs are now authorized to issue their own data-seeking orders to U.S. CSPs. Before the CLOUD Act, CSPs who disclosed customer or subscriber data to foreign governments faced potential civil and criminal liability in the United States unless the foreign government used an MLAT and went through the DOJ.[7] That remains the status quo for most foreign governments, but the CLOUD Act now also permits service providers to comply with orders from QFGs without violating U.S. law or facing civil liability in United States courts.

Key Differences Between Qualifying Foreign Governments ("QFGs") and Other Foreign Governments

	QFG	Not a QFG
A U.S. government has issued a warrant, subpoena or court order to produce data that conflicts with foreign privacy law	The provider can file a motion to quash or limit the legal process if the customer/subscriber is not a U.S. person/resident.	The provider must comply with the U.S. order (unless courts create a common-law comity exception to the SCA).
A U.S. court has ordered the provider not to disclose the existence of the government's request (using 18 U.S.C. § 2705(b))	The provider may tell the QFG (through a designated agency) "of the existence of legal process" seeking the data of one of the QFG's nationals or residents.	The provider may not tell the foreign government that the U.S. government is seeking data belonging to one of its nationals or residents.
A foreign government has ordered a provider to produce customer data or to monitor a customer account	The provider may cooperate without fear of civil or criminal liability.	The provider may face civil and criminal penalties if it cooperates. The foreign government must use an MLAT.

It's a Long Road to QFG Status

Getting recognition as a QFG is a long, demanding and convoluted procedure. The foreign government needs to enter into an executive agreement, have the U.S. Attorney General certify that the agreement meets a long list of criteria, and survive a congressional veto. After these procedures are complete, the executive agreement is certified to satisfy 18 U.S.C. § 2523. A foreign government is then deemed to be a QFG if it both has a certified executive agreement and has additional rules in place that limit its own use of data production orders when they conflict with other countries' laws.

[7] A list of countries that currently have MLATs in force with the United States can be found here.

The first step to becoming a QFG is to enter an executive agreement on data privacy with the United States that meets a list of requirements set out in the CLOUD Act.[8] After the agreement is signed, the U.S. Attorney General needs to certify, with the concurrence of the Secretary of State, that both the foreign government generally and the executive agreement in particular meet the criteria set out in a new section in a new section of the U.S. Code. 18 U.S.C. § 2523. The criteria focus on whether the foreign government has adequate respect for individual rights and civil liberties and adequate laws regarding cybercrime and data privacy. For example, the foreign government must either be a party to the Budapest Convention on Cybercrime or have analogous domestic laws. The foreign government must also have adopted "appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning United States persons."

The Attorney General also needs to certify that the executive agreement satisfies an 18-point checklist of terms and conditions. Key requirements are that the orders will not be used to target U.S. persons or residents, that orders will only be used to combat serious crime, and that there are procedural restrictions on how orders can be issued. The agreement also needs to be reciprocal, meaning that CSPs will not face liability for complying with U.S. orders that would otherwise violate local law.

Once the Attorney General certifies the agreement (with the concurrence of the Secretary of State), she or he has seven days to send the certification and the executive agreement to Congress for a 90-day veto period. These documents are referred to the Judiciary and Foreign Affairs Committees in the Senate and the House of Representatives respectively. These committees have a maximum of 60 days to investigate, hold hearings and issue reports on the certification and the executive agreement.

During the 90-day time period, the Majority or Minority Leader in either house can introduce a joint resolution disapproving of the certification. The structure and even the text of the joint resolution are specified in the CLOUD Act, and it is subject to fast-track procedures by which certain procedural impediments often relied on to delay or defeat a legislative measure are unavailable.[9] If a joint resolution of disapproval passes both houses, the executive agreement is canceled. If no such resolution is passed in 90 days, then the executive agreement and certification go into effect.

Once the foreign government has a certified executive agreement in place, U.S. CSPs may comply with its data production orders. But U.S. courts cannot modify or quash U.S. production orders that conflict with the foreign government's laws unless it is also "qualified," by having two additional laws in place: (a) that the foreign government has an analogous procedure to quash or modify its orders and (b) the foreign government allows service providers to disclose to other qualified governments when the foreign government is seeking customer data in conflict with the other state's law. The table below illustrates these differences with six variations on the *Microsoft* case. It is unclear why these requirements were not included in the Attorney General certification process, and it is strange that their determination appears to be left to the courts when the certification process itself is not subject to judicial or administrative review.

[8] According to the Act's lead Senate sponsor, Senator Orrin Hatch, these criteria are based on a draft agreement between the U.S. and the UK.

[9] These procedures appear to be modeled off of the Congressional Review Act, 5 U.S.C. § 801-02, used to review administrative agency decisions through a similar expedited process.

The Procedure to Certify an Executive Agreement under 18 U.S.C. § 2523

Executive Branch

The executive enters an executive agreement with a foreign government.

The Attorney General (AG) must certify in writing, with the concurrence of the Secretary of State, that:

1a. The foreign country protects civil liberties and human rights (according to defined criteria) and is committed to the "open, distributed, and interconnected nature of the Internet."

1b. The foreign government has adequate laws on cybercrime, has clear laws on how the government collects and uses data, and has mechanisms that make the use of data transparent and accountable.

2. The foreign government has adopted procedures to limit the collection, retention, and dissemination of data concerning U.S. persons.

3. The agreement itself requires all of the following:
   - Orders will not be used to target U.S. persons or residents directly or indirectly.
   - The foreign government will seek information only on its own behalf and not for another state or for the United States.
   - Orders are to be used for combating serious crimes.
   - Orders will be authorized by domestic law, narrowly targeted, based on reasonable and particularized suspicion, and subject to judicial oversight. Orders to intercept data also need to be limited in time and not used if there is a less intrusive alternative.
   - Orders will not be used to infringe free speech.
   - The foreign government will promptly review and securely store data it collects.
   - The foreign government needs to follow FISA-like procedures to segregate and delete data not relevant to law enforcement or safety.
   - The foreign government cannot give a U.S. person's data to the U.S. government unless that disclosure complies with the foreign FISA-like rules and relates to a significant threat to the Unites States or U.S. persons.
   - The agreement needs to be reciprocal, including allowing companies to comply with American orders even if they would otherwise violate local law.
   - The foreign government agrees to periodic review of compliance with the agreement.
   - The U.S. government retains a veto power to say that the agreement does not properly apply to a particular order.

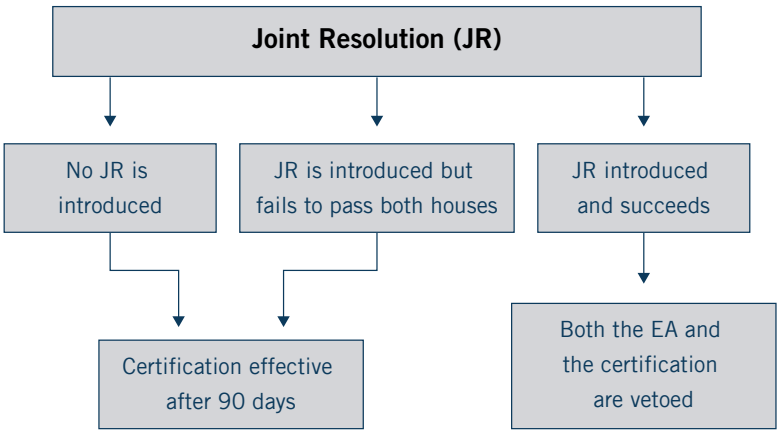
The AG then has seven days to send the certification and the executive agreement to Congress.

Congress

The certification is not effective for 90 days from when the A.G. sends the certification to Congress.

Specified committees in each house have 60 days to consider the agreement, hold hearings, and issue reports.

The majority or minority leader in either house can introduce a joint resolution of disapproval. If they do so, there is an expedited vote with limited debate and the resolution will be fast-tracked in the other house.



Will Non-U.S. Governments Actually Join the QFG Club?

Among the questions most difficult to predict following passage of the CLOUD Act is how many non-U.S. Governments will pursue certified executive agreements or seek to be qualified. Based on consideration of the factors outlined below, there is a good chance that many governments may decline to participate in the new U.S.-driven privacy regime envisioned by the CLOUD Act.

– First, the certification requirements are quite sweeping and strict, and non-U.S. governments may not feel the juice is worth the squeeze. According to Senator Orrin Hatch, these criteria are an "outgrowth" of the "the U.S.-UK bilateral agreement framework," but we do not know how many foreign governments will accept them.

– Second, many of the most likely candidates for QFG status are EU countries and, as set forth above, the provisions of the soon-to-be-effective GDPR may conflict with the CLOUD Act.

Examples Showing the Difference Between Certification and Qualification

	Ireland orders a service provider to produce data prohibited by U.S. law	**The United States orders a service provider to produce data prohibited by Irish law**
Ireland does not have a certified executive agreement with the United States.	The service provider may not comply. Ireland must use an MLAT.	The service provider must comply (unless courts create a common-law comity exception to the SCA).
Ireland has a certified executive agreement but no procedure to quash or does not permit notice to qualifying foreign governments.	The service provider may comply without fear of U.S. liability.	The service provider must comply (unless courts create a common-law comity exception to the SCA).
Ireland has a certified agreement, has a procedure to quash, and permits disclosure to qualifying foreign governments.	The service provider may comply without fear of U.S. liability.	The service provider can file a motion to quash or limit the order (if the customer is not a U.S. person/resident). The provider can also tell the Irish government that the United States has made such a request, even if there is a protective order keeping the request secret.

– Third, the CLOUD Act appears to grant the Executive Branch, in the form of the U.S. Attorney General, broad discretion to enter into executive agreements or pursue certification, which may prompt non-U.S. governments to question the value of investing in executive agreements or the certification process.

– Finally, none on this will happen quickly given that under the CLOUD Act certifications do not become effective until 90 days from when they are sent to Congress.

It is important to highlight that the decision to enter into executive agreements with the United States and to meet the requirements of a QFG will have broader implications given the protective provisions regarding motions to quash or limit are tied explicitly to QFG status under the CLOUD Act.

QFG Status: Greater Direct Access to Data Held by US CSPs

Current U.S. law generally prohibits U.S. providers of communications services and remote storage or processing from disclosing customer data or records unless one of several enumerated exceptions applies. Those exceptions do not include disclosures to foreign governments through legal process. *See* 18 U.S.C. § 2702. Thus, U.S. CSPs are barred from complying with foreign orders to produce customer data unless that request was done using an MLAT through the DOJ.

That remains the status quo for most countries. But the situation changes radically if the country has a certified executive agreement under § 2523 (note that this is a slightly lower standard than being a QFG). In that case, CSPs may now cooperate with the foreign government without facing civil or criminal liability in the United States. Section 4 of the CLOUD Act does this by adding cooperation with orders from countries with certified agreements as enumerated exceptions to existing privacy laws and as defenses to related civil causes of action. (Note that these changes do not *require* service providers to comply with foreign orders; they merely permit them to do so.) In particular, CSPs can now comply with foreign orders to:

– Disclose stored communications, stored data, and customer account information,

– Monitor user communications, including through a wiretap, or

– Install pen registers and tap and trace devices (which track outgoing and incoming phone calls, respectively).

The most surprising thing about this provision, and the one that has drawn the most criticism from privacy groups, is the lack of U.S. oversight into these orders once the country has a certified executive agreement under § 2523. Previously, even data requests from the United States' closest allies had to be made through MLATs and processed by the DOJ. Now they can be made directly to the CSPs.[10] Because the CLOUD Act ignores where data is physically stored, this section opens the door to foreign data seizures, and even wiretaps, on U.S. soil (though the certification procedure requires that the QFG agree to avoid intentionally targeting U.S. persons or residents).

[10] The only oversight mechanism explicitly mentioned in the statute is that executive agreement certifications must be renewed every five years.

Conclusion: Major Questions Remain and Need to Be Monitored

All the parties to the *Microsoft* case agreed that it would be best for Congress, not the courts, to decide how broadly the Stored Communications Act applies. Well, Congress has now done so, giving U.S. law enforcement explicit authority to reach data stored anywhere in the world by U.S. CSPs. That said, the CLOUD Act also leaves some old questions unanswered and raises new ones. These questions and uncertainties will directly impact U.S. CSPs and their growing lists of customers and subscribers. Here are five key areas that should be monitored going forward.

1. Under the literal language of the CLOUD Act, motions to quash or limit U.S. legal process are tied to QFG status, and no QFGs currently exist or are likely to exist for at least several months. How will U.S. courts respond? Will they enforce the statute literally and require compliance or will they create a judicial exception?
2. How many countries will pursue certified agreements with the United States or seek to become QFGs? Will foreign governments accept the requirements of § 2523? How active will the DOJ and State Department be in entering and certifying these agreements?
3. How will the potential conflict between the CLOUD Act and GDPR be resolved if at all given the legal obstacles and the wide-spread and increasing concerns of EU member states about privacy and the tech sector?
4. How will courts respond to U.S. orders that conflict with the privacy laws of a non-qualifying foreign government? Will § 2703 be read strictly to require the service provider comply no matter what, or will courts read in a common law comity exception? This was an open question before the CLOUD Act and one the Act explicitly did not address.
5. The definition of a "qualifying foreign government" requires both that the country is party to a certified executive agreement and that the foreign country has conflict-of-laws rules similar to those in the CLOUD Act. The procedure for establishing the former is clear, but who decides the latter? Will it just be for the courts to decide on a case-by-case basis?

Practical Guidance Tips

- **Consult with key members of your Legal and IT teams to assess the potential impact of the CLOUD Act on current and future operations.**
- **If you have not already done so, map your cloud data so you know where your data is stored.**[11]
- **Review your current contracts with CSPs to see what notification provisions are currently in place.**
- **Designate a point person to monitor this area so critical developments can be shared in real time with key stakeholders or decision makers.**

[11] By way of reference, all of the "Big Five" tech giants store data in the EU. Alphabet (Google) also stores data in Taiwan and Singapore and Apple in Singapore and (soon) China. Amazon and Microsoft have data centers all over Europe and Asia — including China, India, Japan, Korea, Singapore, Switzerland, and the UK — as well as in Australia, Canada, and Brazil. And these networks are expanding. Amazon has plans to add Bahrain and Microsoft is adding coverage in the UAE and South Africa.

Contact Us

Ben Barnett
Partner
+1 215 994 2887
ben.barnett@dechert.com

Vernon L. Francis
Partner
+1 215 994 2577
vernon.francis@dechert.com

Jeffrey A. Brown
Partner
+1 212 698 3511
jeffrey.brown@dechert.com

Theodore E. Yale
Associate
+1 215 994 2455
theodore.yale@dechert.com

Dr. Olaf Fasshauer
Partner
+49 89 21 21 63 28
olaf.fasshauer@dechert.com

The views expressed in this article are those of the authors and do not express the views of Dechert LLP or its clients.