Does the Cloud Act give us a glimpse at a template for GDPR-like adequacy decisions in the US?
By Justin Hartley[1]

The Clarifying Lawful Overseas Use of Data Act ("Cloud Act") was passed in 2018 and sought to more efficiently facilitate law enforcement access to data.[2] This was in response to issues with pre-existing U.S. laws like the Electronic Communications Privacy Act ("ECPA") and, more specifically, the Stored Communications Act ("SCA"), that were showing their age when applied to global cloud infrastructure.[3]

The act contains a process to facilitate bilateral agreements between the U.S. and other certifiable nations that authorizes international data transfers to assist law enforcement in fighting serious crimes.[4] Not all nations are certifiable, but those that are will undergo a thorough analysis to determine if that nation "affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection."[5]

This certification process can be adapted and improved to develop an American system for commercial purposes that bolsters privacy protections and functions like the GDPR's adequacy decisions (except not for law enforcement). Through modifying the Cloud Act, looking to the EU's approach to adequacy decisions, and learning from the terms of the U.S. – U.K. executive agreement, we can begin developing a template for how a federal privacy law may approach a system for 'adequacy decisions'. Theoretically, should a U.S. privacy law provide this system, it could generally further information privacy and security practices across the globe, while streamlining some compliance efforts for businesses that transfer data internationally.

Origin and Purpose of the Cloud Act

The Cloud Act was originally enacted to address an issue with the territorial scope, or permissive reach, of the SCA that was implicated in the *U.S. v. Microsoft Corp.* suit of 2018.[6]

In *U.S. v. Microsoft Corp.,* federal prosecutors tried to use a warrant authorized under the SCA to obtain emails and information relating to an individual's account that was associated with a drug trafficking case.[7] Microsoft discovered that some of the materials sought were stored on data servers in Ireland and refused to hand over the information that was stored abroad.[8] The basis for their challenge to the warrant was because U.S. laws are presumed to not be extraterritorial and the SCA did not specify its extraterritoriality.[9] The case was eventually appealed to the United States Supreme Court and, while the case was pending, Congress passed the Cloud Act, which amended the SCA by expanding its jurisdictional scope.[10] Challenges to government orders, like Microsoft's, were mooted by the main

---

[1] J.D. 2020, Santa Clara University School of Law, CIPP/US. This article was published to complete the requirements for the Privacy Law Certificate at Santa Clara University School of Law. Special thanks to Caitlin Mitchell for edits.
[2] Stephen Mulligan, Cong. Research Serv., R45173, *Cross-Border Data Sharing under the CLOUD Act* 1 (2018), available at https://fas.org/sgp/crs/misc/R45173.pdf (hereinafter referred to as "Mulligan CSR").
[3] *Id.*
[4] *See* 18 U.S.C.A. § 2523.
[5] 18 U.S.C.A. § 2523(b)(1).
[6] *See U.S. v. Microsoft Corp.,* 138 S.Ct. 1186 (2018).
[7] *Id.*
[8] *Id.*
[9] *Id.*; *See RJR Nabisco, Inc. v. European Cmty.,* 136 S.Ct. 2090, 2101 (2016).
[10] *See U.S. v. Microsoft Corp.,* 138 S.Ct. 1186 (2018).

provisions of the Cloud Act, which can be broken down into two parts.

First, the act increased the scope of the SCA to be extraterritorial and outlined new limitations on how law enforcement could exercise this ability.[11] The Cloud Act expanded the use of warrants to mirror modern globalization trends by "clarifying" that when U.S. law enforcement requested data through a valid warrant or subpoena it was to be provided, regardless of where it was stored.[12] This provision only applies if U.S. law enforcement has jurisdiction over the entity.

This expansion of the Cloud Act permitted two new challenges to government orders stemming from the SCA: (1) if an order seeks information on a "customer or subscriber" that is not a U.S. person (or U.S. resident); or (2) it would create a "material risk" of clashing with the other nation's laws the receiving party may challenge the order.[13]

Second, the act created a system that allows for bilateral executive agreements between the U.S. and other countries to share data to assist law enforcement in combating serious crimes.[14] These agreements allow foreign governments to seek data *directly* from U.S. tech companies, provided that (1) an agreement is in force, (2) they are not seeking data on a U.S. person, and (3) the request has an adequate basis in the foreign country's law.[15]

Initially, the ECPA prohibited communication service providers from disclosing electronic communications directly to foreign governments.[16] Before the Cloud Act, foreign nations were required to write a 'letter rogatory' or go through the lengthy Mutual Legal Assistance Treaty (MLATs) process to access data possessed by U.S. based tech companies.[17] Executive agreements function as an exception to this prohibition allowing qualified foreign governments an opportunity to directly petition tech companies in the U.S. With an executive agreement in place both the U.S. and the selected government can directly petition tech companies, headquartered in either country, for access to data that is permitted under the agreement.

The Cloud Act outlines a robust process that certifies other nations as an acceptable partner for a bilateral executive agreement.

Requirements and Process for an Executive Agreement

To enter into force, a proposed executive agreement must be certified by the U.S. Attorney General and Secretary of State.[18] These four requirements assess the other nation by looking to see if that nation's government and the proposed agreement:

---

[11] Morrison Foerster, *CLOUD Act: New Legislation Will Overhaul U.S. Laws for Obtaining Data Stored Overseas* (Mar. 26, 2018), https://www.mofo.com/resources/publications/180326-cloud-act.html.
[12] 18 U.S.C.A. § 2713.
[13] 18 U.S.C.A. § 2713(2)(B)(i–ii).
[14] Jim Garland & Alexander Berengaut, *CLOUD Act Creates New Framework for Cross-Border Data Access*, COVINGTON (Mar. 26, 2018), https://www.insideprivacy.com/cloud-computing/cloud-act-creates-new-framework-for-cross-border-data-access/.
[15] Mulligan CSR at 2–3.
[16] *Id.* at 10–11.
[17] *Id.* at 11. The MLAT process is established but slow, taking on average ten months to process a request. A letter rogatory is a letter written by a court of one nation requesting the assistance of a court in another.
[18] 18 U.S.C.A. § 2523(b)(1–4).

1. *"Affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government. . ."*[19]

This first certification requires a rigorous analysis of "credible information and expert input" on specifically listed factors. This analysis looks to: (1) adequate laws on cybercrime and electronic evidence;[20] (2) respect for the rule of law and nondiscrimination;[21] (3) adherence to international human rights obligations;[22] (4) procedures that govern how and who is authorized to seek data under the executive agreement and how they use and share data;[23] (5) mechanisms to provide accountability and transparency regarding collection and use of electronic data;[24] and (6) demonstrates a commitment to promoting and protecting the global free flow of information and the interconnected nature of the internet.[25]

2. *"Has adopted appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning [U.S.] persons. . ."*[26]

This second consideration looks at data minimization practices and demands that potential orders be tailored to minimize collecting data on U.S. persons.[27] Data minimization is the general notion that data collection activities should be limited to precisely what is explicitly relevant and necessary.

3. *The proposed agreement "shall not create any obligations that" limit or force providers to decrypt data.*[28]

The Cloud Act assures that an executive agreement is encryption neutral.[29] This means that the agreement itself cannot be the source of a decryption obligation.[30] However, this does not limit or prevent service providers from willingly assisting in decryption, nor does it prevent the application of decryption requirements stemming from either nation's laws.[31]

---

[19] *Id.* at § 2523(b)(1)(A–B).
[20] *Id.* at § 2523(b)(1)(B)(i).
[21] *Id.* at § 2523(b)(1)(B)(ii).
[22] *Id.* at § 2523(b)(1)(B)(iii)(I–V).
[23] *Id.* at § 2523(b)(1)(B)(iv).
[24] *Id.* at § 2523(b)(1)(B)(v).
[25] *Id.* at § 2523(b)(1)(B)(vi).
[26] *Id.* at § 2523(b)(2).
[27] Nathan Swire, *Applying the CLOUD Act to the U.S.-U.K. Bilateral Data Access Agreement*, Lawfare (Oct. 28, 2019, 2:31 PM), https://www.lawfareblog.com/applying-cloud-act-us-uk-bilateral-data-access-agreement.
[28] *Id.* at § 2523(b)(3).
[29] *Promoting Public Safety, Privacy, and the Rule of Law Around the World, The Purpose and Impact of the CLOUD Act*, U.S. DEP'T OF JUSTICE, 18 (2019), https://www.justice.gov/opa/press-release/file/1153446/download.
[30] *Id.*
[31] *Id.*

4. *The proposed agreement must also abide by numerous procedural and substantive requirements that relate to the orders foreign governments can issue.*[32]

These restrictions and requirements include that the government's order must: (1) not intentionally target US persons;[33] (2) be lawful in the issuing country;[34] (3) identify a specific person or account;[35] (4) be premised on articulable and credible facts;[36] (5) not infringe free speech;[37] (6) be issued to obtain information that helps prevent, detect, investigate, or prosecute a serious crime;[38] (7) minimize access, ensure security for the information sought consistent with section 101 of FISA, and not share the information obtained.[39] In addition, the other government must allow for periodic review to maintain compliance and allow reciprocal rights of data access for the U.S. to the other nation's communication service providers.[40] The U.S. also reserves the right to render agreements inapplicable to orders it concludes are not properly covered under the agreement.[41]

Once the Attorney General certifies a proposed agreement to the above requirements it moves to Congress to be considered.[42] Congress is allowed an opportunity to introduce a 'joint resolution of disapproval' during the mandatory 180-day period before an executive agreement goes into effect.[43] Curiously, this certification process "shall not [be] subject to judicial or administrative review" and lacks transparency.[44]

The Cloud Act's executive agreements require a robust assessment of another nation before they can come into force and are reminiscent of Europe's approach to adequacy decisions under the GDPR.

GDPR Art. 45 - Adequacy Decisions

An adequacy decision is the process by which the European Commission determines if a country outside of the EU offers adequate levels of protection for individuals rights and freedoms over their personal data.[45] If an adequacy decision has been successfully determined with respect to another country, then personal data may be transferred to entities within that country, provided that all other GDPR compliance obligations are met.[46] It is also worth noting that the GDPR's adequacy decisions do not cover law enforcement data exchanges, which is the entire purpose of the Cloud Act.[47]

---

[32] Mulligan CSR at 17–18.
[33] *Id.*
[34] *Id.* To be lawful in the issuing country, they must be subject to review or oversight by a court or similar authority.
[35] Mulligan CSR at 18.
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] 18 U.S.C.A. § 2523(d)(4)(F–H).
[40] *Id.* at § 2523(d)(4)(I–J).
[41] *Id.* at § 2523(d)(4)(K).
[42] Garland, *supra* note 13.
[43] 18 U.S.C.A. § 2523(d)(4)(C).
[44] *Id.* at § 2523(c).
[45] *International Transfers*, European Data Protection Supervisor (last visited May 16, 2020), https://edps.europa.eu/data-protection/data-protection/reference-library/international-transfers_en.
[46] *Id.*
[47] *Adequacy Decisions: How the EU determines if a non-EU country has an adequate level of data protection*, European Commission (last visited May 16, 2020), https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

GDPR adequacy decisions consider how that country: (1) compares to the EU with respect to human rights and respect for the rule of law;[48] (2) provides access to justice;[49] (3) can guarantee it offers an adequate level of protection for personal data equivalent to that in the EU;[50] (4) provides an independent data protection supervision authority that will cooperate with EU member states;[51] (5) provides data subjects with effective and enforceable rights with effective administration and judicial redress; (6) engages in its data processing activities,[52] and (7) the scope of applicable legal standards or legislation to data processing and security.[53]

An adequacy decision is not the sole authorized method for transferring personal data outside of the EU. For instance, a multinational organization can impose binding corporate rules ("BCRs") upon itself that can provide the necessary 'adequate safeguards' to demonstrate GDPR compliance.[54] In addition, transfers without an adequacy decision can also be permitted if there are contractual obligations between the parties that establish adequate safeguards.[55] However, while both of these approaches are acceptable, adequacy decisions streamline the process. A business operating in nations that have received an adequacy decision from the European Commission will benefit from the added business efficiency of avoiding this regulatory burden. Such a business may still consider using BCRs and contractual obligations as a redundancy against liability as adequacy decisions are assessed regularly.

The Cloud Act's executive agreements leave room for the improvement of privacy and security practices in their application which is consistent with the goals of the GDPR's adequacy decisions.

Modifications and Clarifications from the U.S. – U.K. Executive Agreement

Unless Congress passes a joint resolution of disapproval, the U.S. – U.K. executive agreement will come into effect this summer. Because it is the first example of an executive agreement, we can gain some insight into possible ways to improve the Cloud Act.

The agreement designates an authority in each country that will review and approve international orders.[56] Communication service providers that receive orders through this agreement can object to orders with the issuing designated authority.[57] If the objection persists, the provider can petition their nation's designated authority to discuss the matter with the other designated authority.[58] The host nation to the provider ultimately holds some veto rights for orders brought through the agreement.[59] This appears to create a much needed layer of accountability by giving a party interested in protecting its citizens the ability to provide input related to the process.

---

[48] GDPR, Recital 104, *Criteria for an Adequacy Decision*, (last visited May 16, 2020) https://gdpr-info.eu/recitals/no-104/.
[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] *Id.*
[53] *Id.*
[54] *International Transfers*, *supra* note 44 (BCRs authorize transfers that are internal to a single organization even if it is multinational).
[55] *Id.*
[56] Jennifer Daskal & Peter Swire, *The U.K.-U.S. CLOUD Act Agreement is Finally Here, Containing New Safeguards*, LAWFARE (Oct. 8, 2019, 2:33 PM), https://www.lawfareblog.com/uk-us-cloud-act-agreement-finally-here-containing-new-safeguards.
[57] *Id.*
[58] *Id.*
[59] *Id.* The UK may veto information sought in US death penalty cases and the US may veto information sought in cases involving free speech.

There are notification requirements upon the government issuing an order if the subject of an order is believed to be within a country that is not a party to the agreement.[60] This notification will be sent to the country that the individual resides in.[61]

As mentioned above, seeking information on U.S. persons is prohibited by the Cloud Act. This agreement offers a similar reciprocal version of that arrangement by limiting the U.S.'s ability to obtain information on U.K. persons until they leave the U.K.[62] In addition, the agreement allows for some transparency in two ways: (1) challenges to orders can include both nation's designated authorities; and (2) both the U.S. and U.K. are to issue annual reports on their usage of the agreement.[63]

Both metadata and content data can be implicated under the agreement.[64] However, this agreement provides some clarification to the Cloud Act by defining serious crimes, which was previously left open-ended.[65] Serious crimes are those that carry "a maximum punishment of three or more years" imprisonment.[66] This clarification is useful because these international orders are supposed to be restricted to combating serious crimes. Additionally, the agreement outlines how the U.K. should handle any data it acquires on U.S. persons and notify the U.S. of any alterations to this process.[67]

The notions of notice, use limitations, minimization, accountability, and transparency embodied within this agreement are all helpful in adapting the Cloud Act for commercial purposes that can bolster privacy and security safeguards

A Glimpse at a Possible Template for U.S. Adequacy Decisions

While the U.S. Cloud Act is for law enforcement purposes, we can explore how the U.S. may approach a system for adequacy determinations through its executive agreements provision. This discussion must begin with the caveat that these executive agreements facilitate data transfers between governments interested in fighting crime. What this means is that the purpose and justifications for these transfers are vastly different than those which apply to international commercial transfers of personal information. In light of this, references to things like government orders, the individuals subject to these orders, and judicial oversight should be replaced with notions of permissive data processing, authorized uses, and personal information.

Now, should the U.S. ultimately adopt a federal privacy law, it may be worth including a provision detailing adequacy decisions as an approach to authorizing international transfers of personal information. These decisions generally promote information privacy and security practices by enticing other countries to adopt laws, regulations, or norms that protect and safeguard personal information.

Companies operating under adequacy decisions gain the benefit of having their compliance efforts streamlined through regulatory clarity. This also allows companies an opportunity to develop additional layers of protection against regulatory enforcement, with respect to international data transfers. This is through the continued adoption of BCRs and by imposing contractual obligations on processors and service providers, all of which further ensures the privacy and security of data. In addition, if we can establish a trend towards more respectable global privacy and security practices, then the fears that give

---

[60] Daskal, *supra* note 55.
[61] *Id.*
[62] *Id.*
[63] *Id.*
[64] *Id.*
[65] *Id.*
[66] *Id.*
[67] *Id.*

rise to data localization legislation will become moot. Collectively, this can help ensure that we avoid a global landscape full of hindrances to cloud infrastructure.

Ideally, a federal privacy law would establish a national data protection authority ("DPA") within the U.S., or bolster the capacity and regulatory authority of the Federal Trade Commission ("FTC") with respect to these matters.[68] This prospective DPA (or the FTC) should be granted the authority to certify other nations for adequacy decisions that can then be approved by Congress, mirroring the Cloud Act's process.

Unlike under the Cloud Act, U.S. adequacy decisions would not be treaties, but instead regulatory determinations. Once in place, a U.S. adequacy decision could authorize international data transfers in much the same way as the GDPR and permit reciprocal international data transfers.

By extrapolating from and improving upon the Cloud Act's approach to executive agreements we can see that an American DPA could use a certification system akin to that explained below for its own adequacy determinations. The below suggestions are inspired by the requirements for the Cloud Act and the European Commission's approach to adequacy determinations. I have also added considerations that would help adapt the framework for commercial purposes, rather than for law enforcement.

1. That the other nation provides a robust system of substantive and procedural protections for privacy, civil liberties, and personal information. To make this certification consider the input of experts, regulators, and stakeholders on:
    a. Relevant laws that implicate digital storage and security obligations for personal information as well as cybercrime;
    b. The other nation's definition of personal information (or personal data), the basis in their society for notions of privacy, as well as the level of rights, and redress available to data subjects over infractions against their rights;
    c. The extent to which the other nation respects the rule of law, as dictated by adherence to international human rights obligations, provides access to justice, and offers procedures that govern redress for violations of civil liberties and discrimination; and
    d. Whether the other nation applies fair information practices, an approach that is substantially similar, or an approach that is more robust, throughout the life cycle of data.
2. That the other nation generally possesses and enforces procedures that strive to provide lawful data processing of personal information, prohibits unlawful disclosures or dissemination of personal information, and provides regulatory oversight over violations of lawful data processing.
    a. For purposes of this certification, consider principles like a purpose limitation, data minimization, data accuracy, storage limitations, security obligations, and deletion requirements.
3. The other nations approach, stance, and regulatory efforts surrounding encryption, or decryption, and information security obligations.
    a. Including, the history of recent data breaches, government decryption attempts, and any remedial efforts, if any, the country has taken in response to these events.
    b. Consider the accountability measures in place relation to these obligations or access to the judicial system for civil proceedings.

---

[68] Jason Weinstein, *The U.S. Doesn't Have a National Data Protection Authority? Think Again…*, IAPP (Oct. 16, 2013), https://iapp.org/news/a/america-doesnt-have-a-national-data-protection-authority-think-again/.

4. The other nation's willingness to accept, implement, or maintain procedural and substantive requirements with respect to personal information and the adequacy decision. As examples:
    a. The basis for data processing must be lawful in both countries;
    b. The data subjects must have been informed of the processing, the purpose of the processing, and the locations from which processing is to take place;
    c. Data processors must provide notice to data subjects when any changes occur to privacy or security notices, especially when the purpose for collection and duration of retention change; and
    d. That the U.S. DPA (or FTC) will conduct periodic reviews of this adequacy decision and reserves the right to render it inapplicable or void.
5. The level of transparency and accountability the other nation possesses, permits, or requires with respect to data processing activities and government enforcement actions (both regulatory and criminal).

The process can also be improved from the Cloud Act. For instance, a prospective privacy law could impose transparency and notice obligations on data controllers, data processors, and the U.S. DPA. The additional measures levied against the DPA could include a full documentation and publishing of their determinations that invites feedback. This would allow an opportunity for analysis by experts and interested parties.

Additionally, the certification process should require some factors to be mandatory and others to be more heavily weighted when making a determination. This is in contrast to the Cloud Act, which appears to follow a totality of the circumstances test with regards to its numerous factors (related to the first certification).

Conclusion

The Cloud Act provides a glimpse at how the U.S. may approach adequacy determinations of another country for the purposes of cross-border data transfers. This approach mirrors the GDPR's, despite being adverse in nature with respect to the purpose of the laws. Moving forward, it will be interesting to see how these executive agreements evolve (or fail to evolve) with time and if the framework that we are seeing represents an American approach that will ultimately be adopted into laws and regulations that control other sectors.