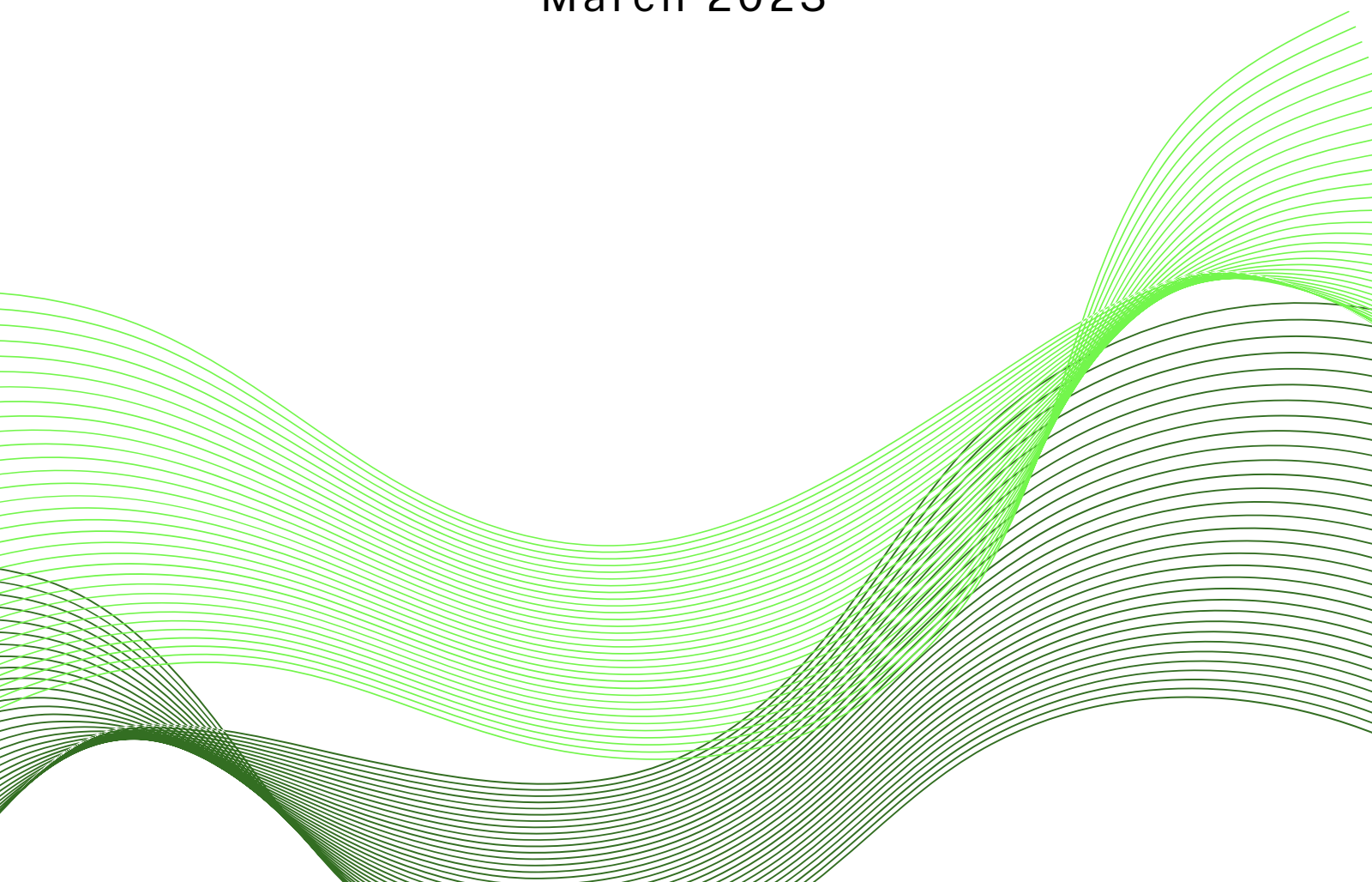
Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

PRIVACY ACROSS BORDERS

Data Localization and Government Access to Data Stored Abroad

Discussion Paper 2

March 2023



Data Localization and Government Access to Data Stored Abroad

March 29, 2023

The Centre for Information Policy Leadership (CIPL) and Tech, Law & Security Program (TLS) have been collaborating on a project regarding data localization policies. As data localization is increasingly gaining traction, we seek to understand the different dimensions of the impacts and effectiveness of these policies. As part of this collaboration—CIPL published a paper on the "real life" business, societal, and consumer impacts of data localization policies and TLS published the present paper on whether data localization measures are legally effective in achieving one of their main ostensible purposes, i.e., to prevent foreign government access to data.

I. Introduction

In this paper, TLS explores one rationale that some proponents of localization have advanced: that localization will insulate companies from foreign governments' ability to legally compel access to their data.[1] We examine not only the legal framework in the United States (U.S.), but also those of other countries, and conclude that legal systems, in general, provide avenues for governments to require companies to respond to data requests, even if data is localized in a different country, and that localization will therefore be ineffective at insulating data from cross-border reach. We begin with a brief (and simplified) overview of applicable U.S. legal principles for law enforcement access to data stored abroad, and then review how other legal frameworks address cross-border data access.

II. Cross-Border Reach Under U.S. Law

a. Personal Jurisdiction

If a U.S. government agency seeks to enforce a data request in court, it must first establish that the company is subject to the court's jurisdiction. This can be a complicated question; for purposes of this paper, we narrow our focus to the concept of "personal jurisdiction."

In the United States, the law of personal jurisdiction has its roots in disputes between litigants located in different states within the country. There are two types of jurisdiction by which a defendant's contacts

[1] Data localization proponents have advanced other justifications for localization measures. For example, a country might feel that requiring data to be stored locally would facilitate access by its own law enforcement agencies, enable the government to better enforce its laws, or to benefit the local economy. Anupam Chander and Uyen P. Le., *Data Nationalism*, 64 EMORY L. J. 677 (2015), https://ssrn.com/abstract=2577947.

with a forum state can bring them into court: general and specific. A court has general jurisdiction when a defendant has "continuous and systematic" contacts that render them "at home" in the forum state. [2] A court has specific jurisdiction over a defendant when it meets certain "minimum contact" requirements.[3] Both general and specific jurisdiction must satisfy due process requirements under the Fourteenth Amendment. In the seminal case of *International Shoe v. Washington*, International Shoe Co. ("International Shoe"), a company with its principal place of business in Missouri and incorporation in Delaware, had salesmen selling shoes in Washington. The Washington state government initiated legal proceedings against International Shoe for unpaid taxes based on the commissions that the salesmen earned in Washington. International Shoe argued that it was not required to pay these taxes because it was not doing business in Washington and for this reason, the court did not have jurisdiction to compel the company to pay the unpaid taxes. The Supreme Court held that the State of Washington did have personal jurisdiction over the Missouri company based on the activities of its sales force within the state, even though the company had no formal offices there. The Court found that as long as a company has "minimum contacts" with the forum state, it is consistent with the Due Process Clause of the Fourteenth Amendment for the state to exercise jurisdiction over the company.[4]

The minimum contacts test balances several factors to determine whether personal jurisdiction over a defendant is proper. This includes whether an entity "purposefully directed" activities to the forum, "purposefully availed" itself of the "privileges and benefits" of the forum, if the litigation was "related to" the entity's activity, and whether it meets the due process considerations of "fair play and substantial justice."[5] U.S. courts also apply this "minimum contacts" analysis to determine whether the U.S. has personal jurisdiction over companies located outside of the U.S.[6]

Many cases since *International Shoe* have found a non-U.S. entity's activities to satisfy the minimum contacts test. In one case involving a hotel company located in Barbados, the United States Court of Appeals for the Third Circuit found that mailing spa brochures to a couple's home in Pennsylvania and making phone calls to schedule the treatment satisfied the minimum contacts test.[7] A more recent case found that a U.S. court had personal jurisdiction over a foreign car manufacturer because of its relationship through its subsidiary in New Jersey, which "markets, distributes, sells, and warrants new vehicles" on behalf of the manufacturer.[8]

---

[2] *Goodyear Dunlop Tires Operations*, *S.A. v. Brown*, 564 U.S. 915, 919 (2011).
[3] *International Shoe v. Washington*, 326 U.S. 310, 316 (1945).
[4] *Id.*
[5] *See Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 475 (1985); *World-Wide Volkswagen Corp. v. Woodson*, 444 U.S. 286, 297 (1980); *Helicopteros Nacionales de Colombia*, *S.A. v. Hall*, 466 U.S. 408, 414 (1984); *International Shoe v. Washington*, 326 U.S. 310, 324 (1945).
[6] *See, also Goodyear Dunlop Tires Operations*, *S.A. v. Brown*, 564 U.S. 915, 919 (2011); *Daimler AG v. Bauman*, 571 U.S. 117, 118 (2014).
[7] *O'Connor v. Sandy Lane Hotel Co.*, 496 F.3d 312, 323 (3d Cir. 2007).
[8] *Rickman v. BMW of N. Am. LLC*, 538 F. Supp. 3d 429, 433 (D.N.J. 2021).

b. "Possession, Custody or Control"

Once personal jurisdiction is established, the question becomes whether U.S. law authorizes the government to compel a party to produce relevant information that is located outside the country's borders. In the U.S., the government took the position that it has the power to compel production so long as the entity has control over the information **and** the U.S. court has jurisdiction over the entity.[9] The U.S. government cited extensive legal precedents to that effect in the *Microsoft Ireland* case.[10] For example, in its brief to the Supreme Court, the U.S. government relied on *United States v. First Nat. City Bank*, which found that "a federal court has the power to require the production of documents located in foreign countries if the court has *in personam jurisdiction* of the person in possession or control of the material."[11] Further, the U.S. government in *Microsoft Ireland* asserted that the Stored Communications Act[12] was enacted with knowledge of "[the principle] that the recipient of a subpoena[13] . . . must produce all specified materials within its control, even if the recipient chooses to store those materials abroad."[14]

In the CLOUD Act, Congress codified this position, which provides:

> A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.[15]

The CLOUD Act does not define "possession, custody, or control." In general, relevant dimensions include whether the entity has the legal ability to direct the actions of the entity holding the data abroad, and whether it has operational or "day-to-day" control of the data.[16]

---

[9] *United States of America v. Microsoft Corporation*, 2017 WL 6205806, at *31-*41 (U.S. 2017); *See also Matter of Marc Rich & Co., A.G.*, 707 F.2d 663, 667 (2d Cir. 1983); § 2456 Subpoena for the Production of Documents and Things—In General, 9A Fed. Prac. & Proc. Civ. § 2456 (3d ed.).

[10] In this case, The U.S. government issued a warrant under the Stored Communications Act (SCA) on Microsoft for a customer's content data. Microsoft refused to provide the data because it stated that the data was stored on its servers in Ireland and that the SCA did not have an extraterritorial application. Microsoft won its appeal in the Second Circuit. The government petitioned the Supreme Court and was granted review. However, this case was mooted due to the passage of the CLOUD Act. *Matter of Warrant to Search a Certain E-Mail Acct. Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197 (2d Cir. 2016), vacated and remanded sub nom. *United States v. Microsoft Corp.*, 200 L. Ed. 2d 610, 138 S. Ct. 1186 (2018).

[11] *United States of America v. Microsoft Corporation*, 2017 WL 6205806, at *14-16 (U.S. 2017) (citing *United States v. First Nat. City Bank,* 396 F.2d 897, 900 (2d Cir. 1968)).

[12] 18 U.S.C. § 2703

[13] Although the case involved a search warrant under 18 U.S.C.A. § 2703, the U.S. government argued that this warrant functioned more like a subpoena and should be treated as such. *supra* note 12 at *14-16.

[14] *Id.* at 32.

[15] 18 U.S.C. § 2713

[16] Justin Hemmings, Sreenidhi Srinivasan, Peter Swire, *Defining the Scope of "Possession, Custody, or Control" for Privacy Issues and the CLOUD Act*, 10 J. Nat'l Sec. L. & Pol'y 631 (2020) https://jnslp.com/wp-content/uploads/2020/05/Defining-the-Scope-of-Possession-Custody-or-Control.pdf.

But what if the country pursuing a data localization mandate were to expressly forbid companies from responding to foreign law enforcement requests (*e.g.*, with a blocking statute)? It is important to note that the drafters of the CLOUD Act were sensitive to the possibility that compliance with a court order could put a company in the position of having to violate another country's laws. The CLOUD Act amended the Stored Communications Act to enable a provider to resist legal process on the ground that compliance would put the provider at "material risk" of violating the laws of a government that had entered into a CLOUD Act agreement with the United States.[17] The court would then make its ruling "based on the totality of the circumstances" and the "interests of justice."[18] The existence of a conflicting legal obligation is, therefore, relevant to a court's "comity analysis" but would not by itself be a legally effective bar.

III. Cross-Border Reach under the Laws of Other Countries

Perhaps not surprisingly, other legal systems also provide for the assertion of jurisdiction over a foreign party based on certain contacts or relationships (commercial, criminal, etc.). To illustrate, a study by Hogan Lovells found that "every single country [examined] vests authority in the government to require a cloud service provider to disclose customer data in certain situations, and in most instances this authority **enables the government to access data physically stored outside the country's borders, provided there is some jurisdictional hook, such as the presence of a business within the country's borders**."[19]

The transparency reports of cloud service providers offer evidence of such cross-border reach. As these providers have repeatedly pointed out, the data hosted on their servers can be distributed across multiple global locations.[20] It is, therefore, likely that government requests for data will require a cloud provider to access data stored in a different country. In fact, these companies routinely receive and respond to government requests for data from all over the world.[21] As these companies make clear in their transparency reports, they provide this information according to applicable civil, criminal, administrative, and other national laws. The number of requests and types of data sought vary by country. For example,

---

[17] 18 U.S.C. § 2703(h)(2)(A)(i-ii)

[18] This "comity analysis" is further spelled out in 18 U.S. Code § 2703(h)(3). Its language reflects U.S. case law on how courts should take into account the conflicting obligations established by foreign law, including blocking statutes. For example, in considering the effect of the French blocking statute, the Supreme Court applied a balancing test. *Société Nationale Industrielle Aérospatiale v. U.S. District Court for the Southern District of Iowa*, 482 U.S. 522, at n. 29 (1987). When applying such a comity analysis, U.S. courts usually find in favor of compelling data in most cases, even after considering foreign interests. The Sedona Conference, Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery (2008), at 17, https://thesedonaconference.org/sites/default/files/publications/WG6_Cross_Border_0.pdf.

[19] Hogan Lovells, A Global Reality: Governmental Access to Data in the Cloud (2012), https://www.hoganlovells.com/~/media/hogan-lovells/pdf/publication/revised-government-access-to-cloud-data-paper-18-july-12_pdf.ashx.

[20] Afiq Fitri, *Where are the hyperscale cloud providers building their data centres?*, Tech Monitor (Mar. 9, 2023, 10:59 AM), https://techmonitor.ai/technology/cloud/where-cloud-providers-building-data-centres.

[21] *Id.*; *See e.g.,* Meta, *Government Requests for User Data*, https://transparency.fb.com/data/government-data-requests/ (last visited Jan. 26, 2023); Google, *Global requests for user information*, https://transparencyreport.google.com/user-data/overview?hl=en (last visited Jan. 26, 2023).

in Microsoft's 2022 Law Enforcement Requests Report Transparency Report, Germany had 6,455 law enforcement requests, India had 610, and the United States had 5,560.[22]

The international prevalence of cross-border data access principles is also evident in the Organization for Economic Cooperation and Development (OECD) *Declaration on Government Access to Personal Data Held by Private Sector Entities.*[23] The Declaration "seeks to improve trust in cross-border data flows – which are central to the digital transformation of the global economy – by clarifying how national security and law enforcement agencies can access personal data under existing legal frameworks." The Declaration identifies "shared principles" that reflect "commonalities drawn from OECD Members' existing laws and practices." In outlining the applicability of those principles, the Declaration states that they "apply to government access to and processing of personal data **in the possession or control of private sector entities** when governments are pursuing law enforcement and national security purposes within their respective territories in accordance with their national legal framework, **including situations where countries have the authority under their national legal framework to mandate that private sector entities provide data to the government when the private sector entity or data are not located within their territory**."

More evidence of cross-border reach can be found in many countries' domestic laws. Recently, the Brazilian Federal Supreme Court, relying on Article 11 of the Civil Rights Framework for the Internet[24], found that Brazilian law enforcement authorities can directly request user data for criminal investigations from companies who have representatives in Brazil, but headquartered abroad. This ruling impacts companies such as Meta, Telegram, Twitter, and Google, which "may be asked in other countries to provide data on consumers who use these platforms in Brazil."[25] Dutch law enforcement agencies rely on Article 126ND and Article 126NG(2) of the Wetboek van Strafvordering (Dutch Code of Criminal Procedure) to request data from a provider who has access.[26] Article 155 of Lithuania's Criminal Procedure Code grants prosecutors the ability to request data from any public or private organization after receiving permission from a pre-trial investigation judge.[27] India's Code of Criminal Procedure provides courts and law enforcement agencies with the authority to compel production of a document that is "necessary or desirable for the purposes of any investigation, inquiry, trial or other proceeding."[28] Further, China can

[22] Microsoft, *Law Enforcement Requests Report*, https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report (last visited Mar. 28, 2023).
[23] OECD, *Declaration on Government Access to Personal Data Held by Private Sector Entities* (Dec. 13, 2022), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487.
[24] LAW NO. 12,965, 2014 (Art. 11), available at https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.
[25] Poder360, *Justiça pode pedir dados de big techs no exterior, diz STF* (Feb. 24, 2023, 3:48 PM), https://www.poder360.com.br/justica/justica-pode-pedir-dados-de-big-techs-no-exterior-diz-stf/.
[26] Wetboek van Strafvordering, 1921 (Art. 126ND, 126NG(2)) (Neth.), available at https://wetten.overheid.nl/BWBR0001903/2023-03-01.
[27] European Judicial Network, *Fiches Belges on electronic evidence*, https://www.ejn-crimjust.europa.eu/ejnupload/DynamicPages/LT%20electronic%20evidence%20fb.pdf.
[28] The Code of Criminal Procedure, 1973 (Chapter VII) (India), available at https://legislative.gov.in/sites/default/files/A1974-02.pdf.

access cross-border data according to Articles 7[29] and 14[30] of its National Intelligence Law. Both articles require organizations to support "national intelligence" work or efforts and apply to U.S. companies operating in China.[31]

The General Data Protection Regulation ("GDPR") similarly contemplates cross-border reach. Article 3(1) provides: "This Regulation applies to the processing of personal data in the context of the activities of an **establishment** of a controller or a processor in the Union, *regardless of whether the processing takes place in the Union or not*." The Court of Justice of the European Union defined what an establishment was in *Weltimmo*: "[an] establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements."[32] Stable arrangements depend on "effective economic activities" and the degree of stability found in those activities. The European Data Protection Board describes what constitutes a stable arrangement:

> The threshold for 'stable arrangement' can actually be quite low when the centre of activities of a controller concerns the provision of services online. As a result, in some circumstances, the presence of one single employee or agent of a non-EU entity in the Union may be sufficient to constitute a stable arrangement (amounting to an 'establishment' for the purposes of Art 3(1)) if that employee or agent acts with a sufficient degree of stability. [33]

Thus, under concepts that are comparable to those under U.S. law, EU data protection agencies seeking access to a foreign company's data would need to show that the company had sufficient contacts or presence in the country to trigger the exercise of jurisdiction under Article 3, which in turn would trigger the agencies' authority to demand information under Article 58.[34]

---

[29] "All organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national intelligence work secrets they are aware of." PRC National Intelligence Law, 2018 (Art. 7) (China), available at https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/.

[30] "National intelligence work institutions lawfully carrying out intelligence efforts may request that relevant organs, organizations, and citizens provide necessary support, assistance, and cooperation." *Id.* at Art. 14.

[31] Murray Scot Tanner, *Beijing's New National Intelligence Law: From Defense to Offense*, Lawfare (July 20, 2017, 11:30 AM), https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense?utm_source=POLITICO.EU&utm_campaign=cbece95283-EMAIL_CAMPAIGN_2023_03_23_12_30&utm_medium=email&utm_term=0_10959edeb5-cbece95283-%5BLIST_EMAIL_ID%5D.

[32] C-230/14, *Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, 2015; The GDPR replaced the Data Protection Directive, but Directive 95/46's concept of "establishment" was retained in GDPR's Recital 22.

[33] European Data Protection Board, *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)* (Nov. 2019), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf.

[34] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), O.J. 2016 (L 119/) Art. 58, available at https://gdpr-info.eu/art-58-gdpr/.

Thus, under the principles discussed above, for a company to avoid the cross-border reach of a foreign government's data requests, it would have to minimize ties with that country (e.g., have no significant physical presence there or avoid directing its services to that country), or ensure that any entity that is subject to that country's jurisdiction is unable to obtain access to the data. In short, a company cannot participate in the global market and avoid assertions of jurisdiction from countries outside of its home market.

IV. Cross-Border Legal Instruments

Government agencies need not rely solely on their national laws to obtain data located abroad; bilateral and multilateral mechanisms exist to facilitate such access. An example of a mechanism that provides governments access to foreign data for law enforcement purposes are mutual legal assistance treaties ("MLATs"). The U.S. is a party to MLATs with dozens of countries.[35] Governments frequently complain of the delays and difficulties in using the MLAT process to access data stored in the United States.[36] In the EU, the e-Evidence regulation, awaiting ratification, is designed to help facilitate cross-border criminal investigations between EU member states.[37]

Additionally, global instruments such as the Budapest Convention aim to harmonize laws and procedures to respond to cybercrime, which often transcends the physical borders of just one country.[38] The Budapest Convention requires its signatories to: (1) criminalize certain cybercrime behaviors in their domestic law; (2) have procedural powers to secure evidence and investigate cybercrime offenses; and (3) facilitate international cooperation in cybercrime investigations.[39] If a country wants access to data located in another country while investigating a cybercrime, so long as each is a signatory to the Cybercrime Convention, the investigating country can obtain that data through mutual assistance.[40]

For the U.S., the CLOUD Act authorizes executive agreements between the U.S. and other countries to acquire data from a global communications service provider for law enforcement investigations. Countries

---

[35] Office of Int'l Affairs, Criminal Division, Dep't of Justice, *Mutual Legal Assistance Treaties of the United States* (2022), https://www.justice.gov/criminal-oia/file/1498806/download.

[36] "Considering the large number of [online service providers] based in the US, judicial authorities were asked to identify the main problems encountered with the MLA process towards competent authorities there. The vast majority (89%) of respondents reported the long time needed for MLA procedures as the most challenging issue encountered in 2021. The same issue had been identified as the most prominent one in previous years, demonstrating that this is a recurring and long-standing challenge for EU authorities." EuroPol, *SIRIUS EU Digital Evidence Situation Report* (2022), p. 47, https://www.europol.europa.eu/publications-events/publications/sirius-eu-digital-evidence-situation-report-2022.

[37] Press Release, Council of the EU, Electronic evidence: Council confirms agreement with the European Parliament on new rules to improve cross-border access to e-evidence (Jan. 23, 2023), https://www.consilium.europa.eu/en/press/press-releases/2023/01/25/electronic-evidence-council-confirms-agreement-with-the-european-parliament-on-new-rules-to-improve-cross-border-access-to-e-evidence/#:~:text=The%20regulation%20creates%20European%20production,subscriber%2C%20traffic%20and%20content%20data.

[38] Convention of Cybercrime, Nov. 23, 2011, ETS No. 185, https://rm.coe.int/1680081561.

[39] *Id.* at ch. 2-3.

[40] *Id.* at ch. 3.

that have a CLOUD Act agreement with the U.S. are able "[to] submit orders for electronic evidence needed to combat serious crime directly to communications service providers, without involving the other government and without fear of conflict with U.S. or the other nation's law."[41] The premise behind the agreement is that both countries "have the authority under their domestic laws to compel production of data held abroad by companies under their jurisdiction."[42] Obtaining a CLOUD Agreement with the U.S. is a difficult process and only two countries (the United Kingdom and Australia) have done so to date, with a third under negotiation (Canada).[43] More countries are interested in CLOUD Act agreements.[44] Further, the EU and the U.S. have resumed negotiations to "facilitate access to electronic evidence in criminal investigations."[45]

The above examples evidence a trend in favor of greater cross-border cooperation to facilitate access to data stored in other countries. Determining whether data stored locally could be accessed by a foreign government must, therefore, include an analysis of the extent to which that data could be accessible through a cooperative international arrangement designed to support law enforcement or similar investigations.

V. Conclusion

In sum, even if a country wishes to pursue data localization measures to avoid foreign government access, it is clear that there are many avenues, whether through domestic laws or international mechanisms, for a foreign government to obtain the data. Data localization measures will likely not be effective to achieve that goal.

[41] Dep't of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act* (2019), https://www.justice.gov/opa/press-release/file/1153446/download.
[42] *Id.* at pg. 6.
[43] Department of Justice, *Cloud Act Resources*, https://www.justice.gov/criminal-oia/cloud-act-resources (last visited Mar. 29, 2023).
[44] "New Zealand is eager for a Cloud Act agreement with the United States, as are some Asian countries." Kenneth Propp, *Has the Time for an EU-U.S. Agreement on E-Evidence Come and Gone?*, Lawfare (June 2, 2022, 1:33 PM), https://www.lawfareblog.com/has-time-eu-us-agreement-e-evidence-come-and-gone.
[45] Statement, European Commission, EU-U.S. announcement on the resumption of negotiations on an EU-U.S. agreement to facilitate access to electronic evidence in criminal investigations (Mar. 2, 2023), https://commission.europa.eu/news/eu-us-announcement-resumption-negotiations-eu-us-agreement-facilitate-access-electronic-evidence-2023-03-02_en.