UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF INTERNATIONAL LAW

Volume 44
Number 4 *Online Edition*

Article 4

2019

Nail in the MLAT Coffin: Examining Alternative Solutions to the Current Mutual Legal Assistance Treaty Regime in International Cross-Border Data Sharing

Philip J. Pullen

Nail in the MLAT Coffin: Examining Alternative Solutions to the Current Mutual Legal Assistance Treaty Regime in International Cross-Border Data Sharing

Philip J. Pullen†

I. Introduction

Pardon me for being one to state the obvious—but, the world is changing. Among the many who do not need that fact reiterated to them are officials in domestic and international law enforcement. Today, where a crime is committed, where a suspect is located, and where the evidence necessary to prosecute him or her exists are all often found in locations throughout all corners of the globe.[1] In navigating this reality, law enforcement agencies around the world

---

† J.D. Candidate 2019, University of North Carolina School of Law.

1 Gail Kent, *The Mutual Legal Assistance Problem Explained*, THE CTR. FOR INTERNET & SOC'Y (Feb. 23, 2015, 1:06 PM), http://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained [https://perma.cc/6XAD-Q6GL].

are forced to reach outside of their jurisdictional bounds to request data from various sources around the world.[2] However, the legal framework that currently exists governing cross-border information sharing—Mutual Legal Assistance Treaties ("MLATs")—is woefully inadequate.[3] As a result, countries have begun to look for workable alternatives to the existing process.[4] The United States in particular has recently proposed legislation which would provide an alternative to the current MLAT regime and allow it to form direct, one-on-one information-sharing agreements with other countries, particularly the United Kingdom.[5]

In this paper, I argue, specifically with respect to the recently proposed 2016 U.S. Department of Justice ("DOJ") legislation, that these sort of MLAT "workaround," cross-border information sharing agreements are an effective alternative to the current MLAT regime. They allow countries like the United States to more efficiently produce and request data from other countries, all the while ensuring adequate safeguards for the protection of human and privacy rights. I first discuss the conditions which initially lead to the MLAT framework, but which have now increasingly made that framework unworkable. I then go on to describe the current MLAT process, discuss its flaws as they exist currently, and argue that solutions like those recently proposed in the United States, including the 2016 DOJ legislation, are workable, alternative solutions to the current process.[6]

---

2 *See id.*

3 Drew Mitnick, *The Urgent Need for MLAT Reform*, ACCESS NOW (Sept. 12, 2014, 5:42 PM), https://www.accessnow.org/the-urgent-needs-for-mlat-reform/ [https://perma.cc/52S2-PD9D].

4 *See id.*

5 U.S. DEP'T OF JUSTICE, LEGISLATION TO PERMIT THE SECURE & PRIVACY-PROTECTIVE EXCHANGE OF ELECTRONIC DATA FOR THE PURPOSES OF COMBATING SERIOUS CRIME INCLUDING TERRORISM (2016), https://www.documentcloud.org/documents/2994379-2016-7-15-US-UK-Biden-With-Enclosures.html#document/p1 [https://perma.cc/94A9-FMXL] [hereinafter DOJ Proposed Legislation].

6 At the time of submission, the U.S. Congress had adopted many of the provisions of the 2016 DOJ proposed legislation in the Clarifying Lawful Overseas Use of Data (CLOUD) Act of 2018. *See* Andrew Keane Woods & Peter Swire, *The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems*, LAWFARE (Feb. 6, 2018, 5:49 PM), https://lawfareblog.com/cloud-act-welcome-legislative-fix-cross-border-data-problems [https://perma.cc/CUA5-BUUW]. The Act was passed in an omnibus spending bill on March 23, and essentially "pave[d] the way for executive agreements—such as the contemplated U.S.-U.K. agreement—to allow foreign governments to request content

II. The Current Climate Surrounding International Cross-Border Data Sharing

Global technological change has reshaped the world in recent years. Whether it be the effort to combat global climate change, or the ability of companies to invest in cheap labor markets and export products throughout the world, technological change is undoubtedly the spark plug that continuously ignites new developments in centuries old establishments and practices. One such area that has been impacted dramatically as a result of this technological change is the area of criminal law enforcement.[7] As advancements in technology allow individuals and countries to extend their reach beyond invisible, national borders, countries are struggling to navigate existing legal frameworks in an effort to catch defendants who commit crimes in jurisdictions where they may, or may not be physically present.[8]

The reason the current legal system is inadequate in allowing law enforcement agencies around the world to catch criminals effectively, is due, in part, to the fact that many crimes are now committed in cyberspace.[9] As a result, evidence of such crimes is generally found on data servers which may or may not be in the territorial jurisdiction of the law enforcement agency charged with investigating, and ultimately prosecuting, the crime.[10] Most of the online service providers—like Google and Microsoft—which maintain the servers for which this evidence is located, are headquartered in the United States, but have offices and store data

---

directly from American providers." *Id.*; *see also* Pete Williams, *Supreme Court Seems Set to Rule Against Microsoft in Email Privacy Case*, NBC NEWS (Feb. 27, 2018, 12:49 PM), https://www.nbcnews.com/politics/supreme-court/gov-t-battles-microsoft-email-privacy-case-supreme-court-n851216 [https://perma.cc/V789-E8JS] (predicting a Supreme Court ruling against Microsoft, as expected from application of CLOUD Act). The Act has many of the same provisions as the proposed DOJ legislation: it amends parts of the ECPA "to allow providers to permit disclosures to certain foreign governments[,]" and allows the president of the United States to enter into agreements with countries that meet a certain set of requirements. Woods & Swire, *supra* note 6 . However, for the purposes of this paper, the CLOUD Act itself is not considered because it adopts many of the provisions of the 2016 DOJ proposed legislation, and therefore my arguments similarly apply.

7 *See* Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security & Rights Issues*, 8 J. OF NAT'L SECURITY L. & POL'Y 473 (2016).

8 *Id.* at 475.

9 *See* Kent, *supra* note 1.

10 Daskal, *supra* note 7, at 475—76.

all over the world.[11] Therefore, law enforcement agencies are forced, when they need to obtain data stored by these companies in gathering information on criminals they are prosecuting, to navigate the international legal system in order to work with other countries, where that data may be physically located, in order to obtain certain evidence.[12] This is a particularly difficult task when considering the country in which the suspect is physically located, the country in which the data is stored, and the country whose law enforcement agency is conducting the investigation, all might be separate from one another.[13] As a result of this dilemma, law enforcement agencies are forced to work with one another, each pursuant to their own domestic laws, in requesting and obtaining information on suspects they are investigating.[14]

III. The Current Legal Framework for International Cross-Border Data Sharing

Currently, however, law enforcement agencies around the world struggle to obtain information on criminal suspects from each other's foreign governments, intelligence services, and law enforcement agencies.[15] This is primarily because the law that governs the handing over of personal online information between an online provider and a law enforcement agency is, traditionally, the domestic law of the country in which the information is physically located.[16] Therefore, in addressing the need of law enforcement agencies to work together in sharing information across borders, countries have traditionally used MLATs.[17] However, as the frequency of these types of modern crimes increases, requests for information between countries has and will continue to increase as well. As a result, navigating the MLAT process in obtaining information for ongoing criminal investigations has proven to be extremely burdensome and time-consuming, and has been viewed as an inadequate solution to

11 Kent, *supra* note 1.

12 *See id.*

13 *Id.*

14 Daskal, *supra* note 7, at 475—76.

15 Kent, *supra* note 1.

16 *Id.*

17 *Id.*

address ongoing and real-time threats.[18] Thus, many countries, including the United States, have begun to develop alternative legal agreements to MLATs in order to more efficiently share information with those countries with whom they share information with most often.[19] One example of such an alternative workaround to the MLAT process is the proposed agreement between the United States and the United Kingdom.[20] The agreement would ultimately "allow law enforcement officials in the United Kingdom to wiretap or directly order companies to hand over user data stored in the United States—and vice versa—without going through formal processes."[21] The U.S. Department of Justice has advocated for the ability to negotiate agreements like the one between the United States and United Kingdom in its 2016 proposal to Congress.[22] As is discussed *infra*, these types of MLAT workaround agreements are beneficial to law enforcement agencies who are straining to meet the challenges posed by modern crimes, and countries around the world, and the United States in particular, should negotiate these types of MLAT workaround agreements with one another.

A. What Mutual Legal Assistance Treaties Are and How They Work

Under the current MLAT system, in order to access any sort of electronic information stored by data service providers, including e-mails, tweets, Facebook posts, etc., a country must abide by a specific MLAT that it has negotiated with the country which physically holds the information the former is attempting to obtain.[23] Since most data service providers are based in the United States, countries looking to prosecute suspects within their own territorial jurisdiction must rely on a MLAT it has formed with the United States in order to obtain information located within the

---

18 *Id.*

19 *Id.*

20 Drew Mitnick, *A Diagnosis: Why Current Proposals to Fix the MLAT System Won't Work*, ACCESS NOW (May 2, 2017, 1:32 PM), https://www.accessnow.org/diagnosis-current-proposals-fix-mlat-system-wont-work/ [https://perma.cc/BSP7-8CC9].

21 *Id.*

22 *See* DOJ Proposed Legislation, *supra* note 5.

23 Kent, *supra* note 1.

territorial jurisdiction of the United States.[24] The long, attenuated process ultimately begins when the foreign law enforcement files a request with its country's own central filing agency.[25] That central filing agency then contacts the U.S. Department of Justice (if seeking to obtain information from a provider in the United States), who works with that country to make sure the request meets U.S. legal standards—that it complies with U.S. domestic law.[26] Following the reception of the request and satisfaction that it does meet the standards of U.S. domestic law, the Department of Justice passes it along to the U.S. Attorney's Office for the district in which the data provider is located.[27] The U.S. Attorney then solicits a magistrate judge to receive a court order, and sends that signed court order to the U.S.-based company.[28] Upon receiving the court order making the request, the company is then ultimately required to send any information along to the foreign law enforcement agency.[29]

B. Issues with the Current Legal Framework

Although the process may appear straightforward on paper, it is has proven to be extremely burdensome to both the U.S. Department of Justice and other foreign law enforcement agencies. This burden is based predominantly on the fact that MLAT requests for information have increased drastically in the past few years.[30] In 2015, the DOJ stated in its fiscal year budget request that "request[s] for assistance from foreign entities ha[d] increased nearly 60%, and the number of requests for computer records increased ten-fold[.]'"[31] This increase in cross-border information requests puts an additional strain on the government entities responsible for both sending and receiving the requests, and as a result the time it takes to fully comply with a MLAT request is burdensomely long.[32] For

---

24 *Id.*

25 *See* Tiffany Lin & Mailyn Fidler, *Cross-Border Data Access Reform: A Primer on the Proposed U.S.-U.K. Agreement*, BERKMAN KLEIN CTR. FOR INTERNET & SOC'Y 1, 2 (Sep. 7, 2017, 3:20 PM), https://dash.harvard.edu/bitstream/handle/1/33867385/2017-09_berklett.pdf [https://perma.cc/N92L-UHY3].

26 *Id.*

27 *Id.*

28 *Id.*

29 *Id.* at 2—3.

30 *Id.*

31 Lin & Fidler, *supra* note 25, at 4.

32 Kent, *supra* note 1.

example, the United Kingdom has reported that requests for cross-border information via MLATs can take over a year—up to 13 months.[33] In addition, "[t]he UN Cybercrime Study of 2013 indicates that most countries 'reported median response times of . . . 150 days for mutual legal assistance requests, received and sent . . . . It is clear that the use of formal cooperation mechanisms occurs on a timescale of months, rather than days.'"[34] This issue is particularly apparent when law enforcement agencies are conducting ongoing investigations, in which they need particular information that not only supports the guilt of a criminal for a prior committed act, but in preventing the commission of future crimes as well.[35]

The issues with MLATs extend far beyond the exorbitant amount of time they take to fulfill. For one, countries around the world have grown increasingly frustrated that "U.S. law essentially determines global practices."[36] Since most data providers reside and operate in the United States, most law enforcement agencies will need to utilize MLATs they have negotiated with the United States in carrying out their investigations, and thus are subject to U.S. data privacy laws.[37] Moreover, determining the exact location of the data can be difficult.[38] Many providers, including Microsoft and Google, store data in various locations around the world in order to protect that data from regional political issues, for cost purposes, or for purposes of speed and efficiency.[39] This is problematic because the data protection law that is applied in determining MLAT requests is the law of the jurisdiction in which the data is stored.[40] Thus, issues related to data privacy and free speech arise when countries request stored online information from another country with substantially different domestic laws and protections than the requesting country.[41]

---

33 *Id.*

34 *Id.*

35 *See* Daskal, *supra* note 7, at 480.

36 Lin & Fidler, *supra* note 25, at 4.

37 Drew Mitnick, *What's Wrong with the System for Cross-border Access to Data*, ACCESS NOW (Apr. 25, 2017, 1:22 PM), https://www.accessnow.org/whats-wrong-system-cross-border-access-data/ [https://perma.cc/5AZ2-XXGL].

38 *Id*.

39 *Id.*

40 *Id.*

41 *See id.*

IV. Current and Proposed Solutions to the Mutual Legal Assistance Treaty Problem

In response to these concerns, countries have taken a number of different approaches. Some countries have begun imposing strict data localization laws, limiting the use of encryption to protect data, and passing new extraterritorial laws which permit their law enforcement agencies to unilaterally circumvent the law of the jurisdiction in which the data is stored, and to ultimately order the provider to hand over the data or face a penalty.[42] Concerns have been raised, and rightly so, about these new techniques, which prevent consistency in cross-border data sharing, do not ensure adequate privacy safeguards of user information, put data providers in a legal stranglehold, and encroach on national sovereignty.[43]

Other, more workable solutions have been raised however. The most satisfactory of these is the use of unilateral agreements between countries themselves, which would permit the parties to the agreement to bypass the MLAT process entirely. The agreement would allow one country to reach out to a data provider located in the other country, which is a party to the agreement, and submit an information request pursuant to the requesting country's own domestic laws, and not the domestic laws of the country in which the provider is located or the information is stored, as was the case under the traditional MLAT regime.[44] Thus, these sort of "workaround" agreements would subject foreign companies to the domestic laws of the country requesting the information in the first place, and not the domestic laws of the country in which the information is actually being stored.[45] Presumably as a result of this new legal mechanism's perceived usefulness, some countries, in addition to the United States and United Kingdom, have begun to draft proposals for new MLAT workaround agreements.[46] For example, the European Union (EU) is currently "reviewing digital evidence rules that would apply to all EU countries, and the Council of Europe is in the early stages of negotiations to grant greater direct access to the countries party to the Convention of Cybercrime

---

42 *Id.*

43 Mitnik, *supra* note 37.

44 Kent, *supra* note 1.

45 *See* Mitnick, *supra* note 20.

46 *Id.*

(Budapest Convention)."[47]

A. The Proposed 2016 Department of Justice Legislation

The U.S. Department of Justice proposed legislation to Congress in July of 2016 that would allow and ultimately permit the United States to engage in negotiating these MLAT workaround agreements.[48] According to the proposal, the United States would be permitted to enter into bilateral agreements with other countries (including the United Kingdom), and U.S.-based companies would be required to provide stored information to law enforcement agencies of countries parties to the agreement pursuant to the requesting countries own domestic law, and not the domestic law of the United States.[49] United States courts would thus not have to act as an intermediary in reviewing, approving, and issuing a court order for every information request made by a foreign law enforcement agency, as is currently the practice under the traditional MLAT regime.[50] Instead, companies like Google, Facebook, and Microsoft, who are headquartered and store information inside the territory of the United States would be subject to lawful requests made for that stored information, pursuant to the requesting country's domestic law.[51] The 2016 draft proposal sets out particular standards other countries must meet before the United States government could enter into such an agreement with them, and it "establishes parameters on what [type of information] the requests can include. For instance, requests must pertain to a serious crime, including terrorism."[52]

The proposed legislation would also amend certain parts of Title III of the Electronic Communications Privacy Act ("ECPA").[53] It would amend the Wiretap Act, Stored Communications Act ("SCA"), and Pen/Trap Statute—all parts of the ECPA—"to allow service providers to intercept, access, and disclose communications content and metadata in response to an order from a foreign government, if that order is pursuant to an executive agreement that

47 *Id.*

48 *See* DOJ Proposed Legislation, *supra* note 5.

49 *Id.*

50 Lin & Fidler, *supra* note 25, at 4—6.

51 *Id.*

52 *Id.* at 4.

53 *Id.*

the Attorney General, with the concurrence of the Secretary of State, has determined, and certified to Congress, meets several statutory conditions."[54] These statutory conditions would be implemented to ensure that the requesting country's domestic law affords substantial protection for the privacy rights and civil liberties of the American public.[55] Included among these particular conditions are: "substantive and procedural laws on cybercrime and electronic evidence; evidence of respect for the rule of law and principles of non-discrimination, and adherence to applicable international human rights obligations; [and] mechanisms to provide accountability and transparency for data collection[.]"[56]

Furthermore, the request of information itself must not infringe on an individual's freedom of speech, it must be subject to review by a U.S. magistrate, judge, or other official, and it must be based on a sound legal justification and articulated facts.[57] Finally, the foreign government must afford reciprocity to the United States by allowing it to submit requests for information pursuant to U.S. domestic law, the foreign government must agree to periodic reviews of compliance, and the requesting country must review for and delete any irrelevant information that was sent over.[58] Ultimately, if the United Kingdom, or any other country for that matter, could not successfully comply with the terms of the executive order, they would still have the option to request information through the MLAT process.[59] However, this particular piece of legislation removes the requirement that the U.S. government *personally* review each new request for information from U.S.-based companies, which has proven to be a primary point of contention regarding the new legislation.[60]

---

54 Memorandum from Peter Kadzik, Assistant Attorney Gen., to The Honorable Joseph R. Biden (July 15, 2016) (on file with author) [hereinafter Memorandum].

55 Lin & Fidler, *supra* note 25, at 5.

56 *Id.*

57 *Id.*

58 *Id.*

59 *Id.* at 6.

60 *Id.* at 5 ("[O]rders do not undergo individual inspection by the U.S. government, making the vetting of countries for the executive agreement [like the one between the U.S. and U.K.] the single guaranteed point of scrutiny.").

B. The Effect of the Proposed DOJ Legislation

It is clear that a workable alternative to the current MLAT regime needs to be implemented, particularly since those situations which give rise to the need for any type of agreement in the first place—where a law enforcement agency of one country is forced to request information from a government or company in another country, outside of its jurisdictional bounds—will only continue to increase dramatically. The proposed 2016 DOJ legislation provides an example of legislation that would permit a country, like the United States, to implement such an alternative. Therefore, in underscoring the advantages and disadvantages of these MLAT workaround agreements as a whole, it is helpful to analyze the advantages and disadvantages of the DOJ legislation in particular, and the power it gives the United States to enter into such agreements.

For now, the DOJ proposed legislation is sufficient as an alternative to the current MLAT system in that it addresses the key weaknesses of the current system. This new piece of legislation would essentially do the following: (1) it would ease the burden on the U.S. government, and like parties to the agreement (e.g. the United Kingdom), in providing and receiving information pertinent to criminal investigations; (2) it would prevent U.S.-based data providers from becoming entangled in legal conflicts which may arise when one country's law enforcement agency demands information that U.S. domestic law would otherwise not permit that company to produce; (3) it would ensure reciprocity for United States law enforcement agencies seeking to obtain information about their own ongoing investigations; and (4) it would create a set of norms and standards that both the United States and the rest of the world can use in formulating such cross-border data sharing agreements, while also preventing data localization and providing adequate safeguards for individual and civil liberties.[61]

First, the most obvious advantage of these MLAT workaround agreements, generally, is that they greatly reduce the burdens that electronic communication service providers, as well as the governments of countries that are party to the agreements, face under the current MLAT system.[62] The DOJ proposal in particular,

61 *See* Memorandum, *supra* note 54, at 1—3.

62 *Id.* at 1—2.

and ultimately the creation of bilateral MLAT workaround agreements themselves, would drastically ease the burden on the governments of the United States and United Kingdom, and like countries, in complying with the ever-increasing MLAT requests for information. This legislation does this by removing the critical barrier of forcing the government in which the service provider is located to effectively scan the request and make sure that it complies with domestic law, which is the hallmark of the MLAT system.[63]

This characteristic seems to be the most contentious, since advocates of these agreements see that element as the clog in the system, while opponents see that element as necessary for ensuring privacy and human rights.[64] However, under the proposed legislation, just because the United States would no longer be responsible for "approving" requests for information from law enforcement agencies in the United Kingdom and other countries it enters into such agreements with, it does not mean that those requests will not still provide adequate safeguards for individual and civil liberties. The proposed legislation would simply replace U.S. domestic law governing information requests with the law of the United Kingdom in this particular area.[65] In addition, the proposed legislation comes with the added safeguard that the applicable U.K. law governing information requests from U.S.-based companies must be cleared by the Attorney General, "with the concurrence of the Secretary of State, to determine and certify to Congress that foreign partners have met obligations and commitments designed to protect privacy and civil liberties."[66] However, maintaining the current system, which puts the burden on the "home" country to give the green light for every request for information that the requesting country's law enforcement agency has submitted, creates an unnecessary middleman in every single transaction.

Second, companies would no longer find themselves caught in the "difficult [legal] position" of receiving a request for data that contradicts U.S. law.[67] Under the current regime, U.S.-based data providers confront situations in which they "[e]ither comply with a foreign order, and risk a violation of U.S. law, or they refuse to

---

63 Lin & Fidler, *supra* note 25, at 4—5.

64 *See* Daskal, *supra* note 7, at 496—97.

65 Lin & Fidler, *supra* note 25, at 7.

66 Memorandum, *supra* note 54, at 2.

67 *Id.*

comply and risk violating federal law."[68] United States Assistant Attorney General Peter Kadzik notes, in his memorandum supporting the proposed 2016 legislation, that "[s]ome countries have [even] begun to take enforcement actions against U.S. companies, imposing fines or even arresting company employees."[69] Under the new legislation, companies would not be subject to both the law of the domestic territory in which they reside as well as subject to the foreign law of the country making the request. They would only need to comply with the law of the country making the request, thus alleviating the legal stranglehold many companies currently face.[70] In addition, under the proposed legislation, companies would have the option of complying with the information request or not, subject to their own determinations.[71]

Third, the proposed legislation, and agreement with the United Kingdom arising therefrom, would ensure reciprocity for the U.S. law enforcement agencies seeking to collect data from providers located in the United Kingdom, or storing information in the United Kingdom.[72] This would alleviate the burden on domestic law enforcement agencies seeking to obtain information pursuant to ongoing investigations.

Finally, the proposed legislation would establish a "framework" to serve as the basis for other similar agreements between both the United States and other countries, as well as between other countries themselves.[73] Assistant Attorney General Kadzik stated as much when he emphasized that this legislation would:

> establish a framework and standards that could be used to reach similar agreements with other countries whose laws provide robust protections of human rights, privacy, and other fundamental freedoms. It could thereby increase protections for privacy and civil liberties globally, as countries seeking to qualify for such agreements would need to demonstrate that their legal systems meet these requirements.[74]

---

68 *Id.*at 1.

69 *Id.*at 2.

70 Lin & Fidler, *supra* note 25, at 7.

71 *Id.*

72 Memorandum, *supra* note 54, at 3 (highlighting that the proposed legislation would "[ensure] reciprocal access to data for U.S. investigations").

73 *Id.* at 2.

74 *Id.*

However, many civil liberties groups, including the American Civil Liberties Union ("ACLU"), Human Rights Watch, and Amnesty International, argue that these agreements, and this piece of legislation in particular, do not go far enough in protecting individual privacy and civil liberties.[75] However, safeguards do exist in the proposed legislation which require the Attorney General and Secretary of State to certify that the country with which the United States enters into an agreement provides certain safeguards and meets certain requirements. It provides that any future agreements could be modified or extended based on the particular requirements and domestic laws of the countries with which they are entered.[76]

Without a basis for creating a workable alternative to the currently unsustainable MLAT regime, a vacuum exists where countries, unable to meet or tolerate the demands of the current MLAT system will, and have already started to, revert to solutions that substantially reduce protections for civil liberties.[77] One example of such a situation is the fact that certain countries, like Russia and China, have begun implementing data localization laws which *require* companies to physically store their data in that particular country's jurisdiction.[78] United States—based companies could instead store their data here in the United States and be subject to the legal requirements of a foreign government with whom it has already cleared as ensuring that their disclosure laws maintain adequate safeguards for civil liberties. The alternative would be a situation where these "data localization laws" are passed and United States—based companies are forced to comply with the domestic law of countries that do not provide such adequate safeguards.[79]

The former is simply a more viable alternative than the latter, both in terms of privacy and efficiency. As one scholar notes, although the privacy protections afforded by other countries with whom the United States negotiates these agreements might not rise to the same standard as that articulated in the Fourth Amendment.[80]

---

75 Lin & Fidler, *supra* note 25, at 7.

76 Memorandum, *supra* note 54, at 2.

77 *Id.*

78 *Id.*

79 *Id.*

80 Andrew Keane Woods & Peter Swire, *The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems*, LAWFARE (Feb. 6, 2018, 5:49 PM),

But the Fourth Amendment should not be the benchmark since the alternative is exactly this sort of "data localization" in countries which are plummeting in the opposite direction of ensuring the privacy rights of the Fourth Amendment. "As compared to that world[,]" he notes, this proposed legislation "offers privacy advocates quite a lot."[81]

Another concern has been raised about presidential powers. Specifically, what happens when the president of the United States, who would have the power under this legislation to enter into these bilateral MLAT workaround agreements, negotiates agreements with some countries but not others.[82] This would leave some of the world's biggest markets, such as India and Brazil, in the cold and would incentivize them to mandate localization.[83] However, this is a risk inherent to any bilateral workaround agreement.[84] It is safe to assume that world leaders, and the U.S. president in particular, would do all in their power to negotiate agreements with countries with whom U.S. law enforcement agencies most need information. A further solution is to permit the United States to negotiate these agreements with specific law enforcement agencies of countries, and not the country themselves.[85] This negotiation might serve as a more "streamlined approached," however, it is clear that while there are still wrinkles, these MLAT workaround agreements are the best alternative to the current system. The 2016 DOJ proposed legislation in particular, is a step in the right direction.

V. Conclusion

Ultimately, there is still work left to be done, but the 2016 DOJ proposed legislation is the best alternative to the current MLAT—regime. One that has proven incapable of meeting the demands of law enforcement agencies around the world. This proposed legislation, which would allow the United States to enter into a bilateral agreement with the United Kingdom and other countries, serves as an illustrative example of the advantages and drawbacks

---

https://lawfareblog.com/cloud-act-welcome-legislative-fix-cross-border-data-problems [https://perma.cc/U94R-LQWC].

81 *Id.*

82 *Id.*

83 *Id.*

84 *Id.*

85 *Id.*

of these types of MLAT workaround agreements. While there is still room for improvement, among the many different things this piece of legislation does, it establishes a framework for other countries to use in drawing up their own bilateral agreements with the United States and others. One thing, however, is clear—something needs to be done to replace the current MLAT regime. One which has proven to be incapable of meeting the information sharing demands of law enforcement agencies in the twenty-first century. These MLAT workaround agreements appear to be the most viable alternative.