# **RE-ENGINEERING THE MUTUAL LEGAL ASSISTANCE TREATY PROCESS**

Peter Swire[[1]](#footnote-1)\* & Justin D. Hemmings[[2]](#footnote-2)\*\* **TABLE OF CONTENTS**

I. Introduction

II. History of MLATs

* 1. Letters Rogatory and the History of MLATs
     1. Seeking evidence across state lines
     2. Seeking evidence across national borders
  2. MLATs Today

III. The Importance of MLATs After the Snowden Revelations

A. Factual Changes Leading to the Increased Importance of MLATs

* + 1. The trans-border nature of cyber-crime and cyber-security investigations
    2. Why encryption drives law enforcement to seek records in the cloud, by use of MLATs
    3. More efficient MLATs can counter the perceived risks of strong encryption

B. Challenges Facing Non-U.S. Requests for U.S. Evidence

* 1. The Effects of MLAT Problems on Localization and Other Internet Governance Issues
  2. Conclusion: MLATs as Synecdoche

IV. Methods for Making the Current MLAT Process Faster, Better, and Cheaper

A. Increase Resources to the Office of International Affairs

B. Streamline the Number of Steps in the MLAT Request Process: Creating an MLAT Rocket Docket

C. Streamline Provision of the Requested Records Back to the Requesting Country

D. Others Steps to Increase Efficiency of the MLAT Process and Demonstrate the U.S. Government’s Commitment to Effective Practices

V. Re-Engineer the MLAT Process

A. A Streamlined MLAT Program Similar to the Visa Waiver Program

* + 1. The analogy to the Visa Waiver Program
    2. Assessing the analogy to the Visa Waiver Program
    3. The Fourth Amendment and related issues

B. Scaling the Use of Joint Criminal Investigations – the Online Dating Service Analogy

1. An Internet solution to an Internet problem

2. The need for little or no legislative or treaty change to improve MLAT- type requests

3. Financial considerations

* + 1. Institutional considerations, including confidentiality

VI. Conclusion

1. **Introduction**

Mutual Legal Assistance Treaties (MLATs) have long been an obscure specialty topic for international lawyers. This article contends that MLATs today are emerging as a key component of multiple legal and policy debates in the wake of the revelations by Edward Snowden that began in 2013. Drastically improving the MLAT process has become important, not only for accurate adjudication in individual cases, but also for supporting a globally open and inter-operable Internet against calls for data localization and institution of other stricter national controls on the Internet.

Part I introduces the relevant history, including the first MLAT in the 1970’s to investigate international crimes such as drug trafficking, money laundering, and terrorism. Part II explores the growing importance of cross-border evidence requests over time, spurred by globalization and the combined effects of cloud computing, the growing use of encryption, and law enforcement’s consequent increased need to seek e-mails and other stored records held in other countries. Since the Snowden revelations, delay in MLAT requests have become a rationale for laws that would require data to be stored locally rather than transported across the Internet. Such localization proposals implicate fundamental issues of global Internet governance, so that solving the MLAT problem becomes a key aspect of avoiding splintering the Internet into national fiefdoms. Improving the MLAT process also provides an important alternative to the current advocacy by the FBI and other law enforcement authorities for limits on effective encryption, such as providing law enforcement with access to encryption keys to devices. Where an MLAT request provides access to the plain text of communications at the server level, then the law enforcement case for key escrow is correspondingly weaker.

Drawing on the recommendations of President Obama’s Review Group on Intelligence and Communications Technology, Part III analyzes a number of short- and medium-term policy changes that could make the current MLAT process faster, better, and cheaper. Notably, the U.S. Department of Justice needs greater funding for its MLAT activities, and the U.S. should create a “rocket docket” where prosecutors and magistrates develop expertise in the often-arcane details of MLAT orders, in order both to process legitimate requests more quickly and to assure protection of privacy and human rights where the request does not comply with the Fourth Amendment or relevant law.

Part IV tackles the longer-term challenge of how to re-engineer MLATs to address continuous growth in the volume of international communications and the need of law enforcement to seek evidence across national boundaries. Merely increasing funding to DOJ and processing each request more quickly will not scale to this long-term growth. The paper proposes two conceptual approaches to the re-engineering challenge, both building on existing analogies. First, the Visa Waiver Program provides an analogy for a streamlined MLAT program. As international travel increased over time, the old practice of an individual visa interview became unsustainable. Since 1986, citizens of eligible countries (38 to date) face a greatly streamlined process for visiting the United States. Applied in the MLAT context, due to the analogous globalization of cross-border evidence, the idea is that eligible countries, with high-quality procedures for seeking evidence, would face a streamlined process for gaining evidence in the U.S. The fact that the Visa Waiver Program has operated successfully over time, with strict-yet-manageable criteria for country eligibility, suggests that MLAT stakeholders might fruitfully explore a streamlined MLAT process that learns from the visa waiver precedent.

The second re-engineering concept builds on the long-accepted practice that two jurisdictions can conduct a joint investigation, with law enforcement in Country A seeking evidence in Country A, while law enforcement in Country B seeks evidence in Country B. The main challenges are to find a partner (for the joint investigation), and then to determine that the partner is likely to be a good fit and willing to engage. The closest analogy we have found turns out to be an online dating service – use the Internet to make the match and trade enough information about the partner to have confidence in the fit. The paper suggests a number of lessons for how this joint investigation dating service might work. As with the visa waiver precedent, more research would be needed with MLAT stakeholders to prove the concept and create details about how the service might operate.

In short, this paper explains why the MLAT process matters far more today than in the past, short- and medium-term reforms to address the immediate problems, and two conceptual structures for longer-term re-engineering of the overall system. The paper seeks to stand on its own to advance the state of thinking about these issues, and to propose paths for future research and stakeholder engagement.

**II. History of Mutual Legal Assistance Treaties** Part 1 examines the history of the MLAT and its legal predecessors, notably including letters rogatory, and then describes current procedures for MLAT requests. **A. Letters Rogatory and the History of MLATs** To set the context for modern requests to use the MLAT process, we examine the history for seeking evidence across state lines within the United States, and also across national borders. Historically, letters rogatory were the principle mechanism for sharing evidence between jurisdictions.[[3]](#footnote-3) As the U.S. State Department explains, “letters of rogatory are the customary legal means of obtaining judicial assistance from overseas in the absence of a treaty or other agreement.”[[4]](#footnote-4) These are requests from the courts in one country to courts of another country that “if done without the sanction of the foreign court, could constitute the violation of that country’s sovereignty.”[[5]](#footnote-5) Notably, letters rogatory have been used for service of process and obtaining evidence where permitted by the laws of the foreign jurisdiction. Letters rogatory have relied on principles of comity, or respect for the foreign sovereign, rather than an assertion that the jurisdiction seeking the evidence has a legal right to the evidence. To this day, letters rogatory are signed by a judge seeking the evidence, and they are customarily transmitted via diplomatic channels.[[6]](#footnote-6) Even in the modern age where communications travel instantly via e-mail rather than sailing ship or steamboat, the State Department warns that they are slow and can take a year or more to succeed even where the foreign jurisdiction approves the request.[[7]](#footnote-7)

**1. Seeking evidence across state lines.** In considering how to speed up access to evidence held in other nations, the experience within the United States shows long-standing obstacles to speedy and efficient access even across state lines. Historically, letters rogatory applied if a Texas court, for instance, sought evidence held in another state such as Connecticut. Texas, as a separate sovereign, could not order actions within Connecticut, so a Texas court would issue a letter rogatory to a judicial officer in Connecticut requesting the information be shared. Inside the U.S., this approach based on comity began to shift to legal authority in the 1920s and 1930s as the Uniform Foreign Depositions Act (UFDA) began to see widespread adoption.[[8]](#footnote-8) For the thirteen states that adopted the UFDA, “any mandate, writ or commission . . . issued from any court of record” could be used to compel a witness to appear and testify under the witness’s state rules and procedures.[[9]](#footnote-9) Civil litigants in particular were assured under the UFDA that a different state’s court would assist them in discovery, rather than having to rely on that court’s uncertain and often delayed judicial cooperation.[[10]](#footnote-10) However, even under the UFDA there was still a large amount of judicial oversight and intervention required, and letters rogatory were still often required to obtain evidence from another jurisdiction. The Uniform Interstate and International Procedures Act (UIIPA) attempted to modify and expand the UFDA in 1962, but saw little acceptance from states.[[11]](#footnote-11) In 2007, the Uniform Law Commission issued the Uniform Interstate Depositions and Discovery Act (UIDDA) as a way to streamline the process.[[12]](#footnote-12) Thirty-three states so far have adopted the UIDDA in some form, removing their need for letters rogatory in interstate discovery.[[13]](#footnote-13) However, some states (such as Texas and Connecticut) continue to rely on letters rogatory as the means for conducting out-of-state discovery.[[14]](#footnote-14)

For federal courts, operating under the single sovereignty of the United States, issuing out-of-state subpoenas is simpler. Federal Rule of Civil Procedure 45 describes the process necessary for issuing a subpoena in a different state than the one where the trial is taking place.[[15]](#footnote-15) As long as the subpoena is issued from the U.S. District Court where the evidence is located or the deposition will take place, then an authorized attorney on the pending trial may issue the subpoena without additional court involvement or assistance from local counsel. Rule 45 has become the model for the UIDDA. States that have enacted the UIDDA allow litigants to use a subpoena issued by a court in the trial state to obtain discoverable materials from another state that has adopted the UIDDA. The foreign subpoena is then replicated in a localized subpoena issued by a clerk in the court where the discoverable material is located and then served locally. The terms of the localized subpoena must be identical to the foreign subpoena and contain all relevant contact information. Discovery that takes place in a foreign jurisdiction, however, must comply with all local rules. Therefore, if a trial takes place in State A, but a witness is to be deposed locally in State B, the deposition must comply with State B law. Similarly, motions to quash, enforce, or modify the subpoena must be brought in State B and are governed by State B law.[[16]](#footnote-16) This process not only reduces the time to obtain evidence in foreign jurisdictions, but also reduces the costs of litigation. Out-of-state litigants need not obtain additional counsel local to the discovery state and pay for additional discovery actions in order to obtain evidence. Principles of state sovereignty are still preserved as well since all discovery and accompanying motions and procedures are governed by local state law, not the trial state’s law.

By contrast, those states that have not yet adopted the UIDDA have a longer and more involved procedure. For example, Texas law still requires any person desiring to depose a Texas resident for the purpose of a foreign state action to submit a letter rogatory to the witness’s local Texas court.[[17]](#footnote-17) The local court will then, if appropriate, issue a deposition subpoena under Texas Rules of Civil Procedure. Any issues with the subpoena must be addressed in the issuing Texas court consistent with Texas law. While local counsel is not required in order to process these subpoenas, the process still requires communication between both courts and judges.

**2. Seeking evidence across national borders.** While the Uniform Law Commission has spent the past hundred years working on reforming the system within the United States, international information sharing relied on principles of comity and letters rogatory up until 1977.[[18]](#footnote-18) In 1885, Congress enacted “An Act to Prevent Mis-Trials in the District and Circuit Courts of the United States, in Certain Cases,” which in part authorized U.S. circuit courts to respond to foreign subpoenas in civil actions where the foreign sovereign was a party to the case.[[19]](#footnote-19) In 1948, Congress broadened this Act by removing the sovereign party requirement and including criminal as well as civil acts.[[20]](#footnote-20)

However, as the U.S. began to investigate coordinated international crimes like drug trafficking, money laundering, and terrorism, it faced an increasing need for coordinated information sharing. In 1977, the U.S. entered into its first MLAT with Switzerland in an effort to investigate accounts protected by Swiss banking secrecy laws.[[21]](#footnote-21) This treaty initially required the same standard of “dual criminality” used in extradition treaties, though Switzerland later issued an addendum allowing for information sharing related to U.S. stock trading offenses.[[22]](#footnote-22) Since then, the U.S. has entered into an additional fifty-five MLATs with various countries, including every member of the European Union, and has used these treaties to investigate crimes of money laundering, drug trafficking, terrorism, and international cybercrime.[[23]](#footnote-23) The U.S. continues to negotiate further MLATs with other foreign countries, and has signed and ratified the Inter-American Convention on Mutual Legal Assistance of the Organization of American States.[[24]](#footnote-24)

While an improvement over letters rogatory, MLATs suffer from many of the same issues that the UIDDA addressed. Information sharing is not immediate nor absolute. While a low threshold, the investigating party must still prove it has reasonable suspicion that a crime has been committed within its jurisdiction in order to obtain evidence through the MLAT procedure. Moreover, those requests remain subject to domestic law, such as Fourth Amendment protections against unreasonable search and seizure in the United States. Lastly, while these treaties do create an international law obligation among their signatories, the process itself still requires multiple levels of diplomatic and legal oversight, and the requests for information can be answered at the discretion of the requested party. Consequently, the process remains slow and cumbersome, despite its improvement over the previous letters rogatory.  
 **B. MLATs Today**

Today, MLATs are used frequently for various types of requests, but this paper will focus primarily on the particularly resource-intensive electronic evidence request. While MLATs are often bilateral treaties (except for the multi-lateral treaty between the U.S. and the European Union’s fifty-six member countries in 2010), the process is essentially the same across treaties. When a foreign law enforcement or investigative body determines that it requires access to electronic evidence held under U.S. jurisdiction, such as evidence on servers or computers in the U.S., it files a request with its designated central processing agency. Each treaty designates one point of contact for MLAT requests within each country; the U.S.’s main point of contact is the Department of Justice’s Office of International Affairs (OIA).

Once the request is given to the foreign central authority, that authority makes sure the request is formatted in compliance with the requirements of the relevant treaty. Requests usually include: the name of the authority conducting the relevant proceeding; a description of the subject matter or nature of the proceeding, including any specific charges; a description of the evidence sought along with an explanation for why it is needed; identifying information for whatever individual or entity has control of the evidence, including who should be served with a warrant and where; and a description of any particular procedure to be followed in executing the request.[[25]](#footnote-25) That request is then sent to OIA, who will iterate with the requesting body to make sure the format of the request is correct and that it contains all necessary information.

OIA then works with a U.S. Attorney, who will take the request to a local magistrate judge for review. The office of the U.S. Attorney decides how to prioritize the request, and may place a higher priority on local investigations than requests to assist investigations from a distant jurisdiction, which often does not implicate any local victims. The U.S. Attorney’s office, once it reviews the request, and if it deems appropriate, then places it on the court’s docket, where it is generally placed in line and treated equally with other matters. Any federal judge may review a request to be served in any part of the United States, although generally requests are processed either in D.C. or in the local district where the evidence in question is contained. The reviewing court must then determine whether: (1) the terms of the relevant treaty prescribe specific requirements for producing evidence; (2) the Federal Rules of Procedure and Evidence apply; or (3) the MLAT requires some combination of the two. The court may also verify that the request complies with the specified practices and procedures of the requesting country, but only if they are consistent with U.S. law, including rules of privilege.[[26]](#footnote-26) Lastly, the court must verify that the request complies with U.S. law, including the Fourth Amendment and Fifth Amendment rights of the party or entity in control of the evidence requested. Any deficient requests are rejected, and must go through another round of iterations between the OIA and the requesting country in order to repair the request before it is resubmitted. Repaired or resubmitted requests are given no special priority over other matters before the court.

Once the request has been approved, it can then be served locally on the entity controlling the evidence, in the same way that any Federal warrant is executed. The evidence is then collected and sent back to OIA. OIA then sends the evidence to the point of contact in the requesting country, who then provides it to the investigative team. On average, this process takes ten months to complete for valid and executed MLAT electronic evidence requests.[[27]](#footnote-27)

As discussed further below, multiple factors contribute to a lengthy response time to many MLAT requests. First, foreign countries often have difficulty tailoring requests to comply with US law. The iterations in conjunction with OIA and their U.S. Attorney take time, and every additional iteration adds significant time to the overall process. Second, the lack of prioritization and specialization within the US Attorneys’ offices and the courts reviewing the requests contributes to the significant lag time. In addition, a lack of staff and resources within OIA for processing an ever-increasing number of requests also contributes to the long processing window.

As pointed out by Woods in his report *Data Beyond Borders: Mutual Legal Assistance in the Internet Age*, there are five goals for MLAT reform that are broadly agreed upon by stakeholders.[[28]](#footnote-28) First, MLAT requests should provide access based on more than a mere assertion of wrongdoing and in proportion to the need demonstrated. In other words, access to data through MLATs should be both justified and proportional. Second, the process must protect human rights. Favoring narrowly tailored requests will help avoid the use of MLATs to suppress freedoms of expression and privacy, and greater scrutiny of broader requests will curb attempted abuses. Human rights concerns should also remain a valid basis for the rejection of an otherwise facially valid MLAT request. Third, entities responding to MLAT requests must be transparent about the process and share information on the number of requests and the types of data requested. Transparency will allow for an ex post address of abuses of the MLAT process by those who may not otherwise know they have been harmed. Fourth, the process must be made more efficient as previously discussed. And fifth, reforms must be scalable as the number of MLAT requests, and electronic evidence requests in particular, continue to grow.  
**III. The Importance of MLATs after the Snowden Revelations** The bland term “Mutual Legal Assistance Treaty,” and the unlovely acronym of MLAT, sound appropriate for an unimportant legal topic. Our view, however, is that MLATs are shifting from an obscure specialty issue to a key component of international law enforcement, as well as central to international debates about the structure of the Internet. This Part emphasizes two factual reasons why MLATs are becoming more prevalent – the necessarily international nature of much cyber-crime and cyber-security, as well as the decisive role of increasing encryption on the need for law enforcement to use MLATs. As the importance of MLATs increases, non-U.S. access to e-mails and other records held in the United States becomes far more important. The obstacles to non-U.S. access thus correspondingly become more important. Where non-U.S. law enforcement cannot gain access to records in the U.S., pressure grows for data localization laws – holding e-mail and other records about residents within that country, contrary to the long-standing norm that data flows freely across national borders on the Internet. Even more broadly, as a senior U.S. official told us,[[29]](#footnote-29) MLATs become a “synecdoche” (a part standing for the whole) of non-U.S. frustration with international data flows and surveillance in the wake of the Snowden revelations. This Part explains the emerging importance of the MLAT issue, before turning to possible reforms later in the Article.  
 **A. Factual Changes Leading to the Increased Importance of MLATs** We emphasize two factual changes that are leading to the increased importance of MLATs: (1) the trans-border nature of many cyber-crime and cyber-security investigations; and (2) the reasons why increased use of encryption shifts law enforcement from real-time wiretaps to access to stored records in the cloud, often stored in other countries.

**1. The trans-border nature of cyber-crime and cyber-security investigations.** Even before the Snowden revelations began in 2013, MLATs were becoming more important due to the trans-border nature of many cyber-crime and cyber-security investigations. In the physical world, the thief and the victim are typically in the same country, so there is rarely any need to seek records abroad. On the Internet, by contrast, data breaches and other cyber-crime often involve a foreign perpetrator and a domestic victim. Law enforcement thus far more often has reason to seek records abroad while tracking down criminals. Indeed, the experience of one of the authors (Swire) is that major spam operations that target U.S. individuals have shifted over time from domestic to foreign;[[30]](#footnote-30) the ability to track down perpetrators is high enough within the U.S. that it is only lucrative for spam rings to operate from overseas.

A similar pattern exists for cyber-security. After commercial use of the Internet began in the 1990’s, U.S. law enforcement succeeded in getting legal changes, such as nationwide service of process for federal investigations, that enable relatively effective investigations into the source of attacks from within the country. The focus of effort thus has shifted over time to methods for detecting and countering cyber-attacks that originate from, or are routed through, other countries. MLATs are one tool for gaining evidence about such attacks.

**2. Why encryption drives law enforcement to seek records in the cloud, by use of MLATs.** The increasing use of encryption for on-line communications is a strong accelerator of this trend toward law enforcement seeking evidence from abroad. The reasons are set forth in a 2012 article by Swire called “From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud.”[[31]](#footnote-31) The central point is that encryption makes traditional wiretaps far less likely to be effective; in the absence of wiretaps, law enforcement is driven to the place in the system where data is unencrypted. For e-mails and many other forms of electronic evidence, that place turns out to be the cloud. For many non-U.S. law enforcement investigations, the cloud turns out to be a server in the United States. The way to gain access to that server is through an MLAT.

For decades, law enforcement could use telephone wiretaps in their investigations, and the telephone was the leading technology for remote communications. As telephone technology changed, the United States required telephone carriers to make their systems “wiretap ready” under the 1994 Communications Assistance to Law Enforcement Act (“CALEA”).[[32]](#footnote-32) Today, voice calls through the traditional switched-network telephone network, or for Voice over IP (VOIP) services that inter-connect with that network,[[33]](#footnote-33) retain this obligation to enable a wiretap when served with the appropriate court order.

Remote communications have changed, however. When CALEA was enacted in 1994, Congress created an exception for what at that time was a small fraction of communications – “information services,” notably including Internet communications. This exception meant that hardware and software used for the Internet did not have to meet the “wiretap ready” requirements. Exporting of strong encryption, and use of it with other countries, became generally legal in 1999, but actual adoption was initially lower than expected for email and other Internet actions.[[34]](#footnote-34) For unencrypted communications, law enforcement could intercept the message between sender and recipient. For instance, law enforcement could go to the local Internet Service Provider to intercept Internet traffic going to a local subscriber. For international communications, this meant that a country could generally do a wiretap if either the criminal suspect or victim was in the jurisdiction.

The obstacles to a successful wiretap became much higher by the time of the 2012 article, and the problems have accelerated since Snowden. The earlier article documented a wide range of Internet communications that were being routinely encrypted by 2012.[[35]](#footnote-35) By that time, for instance, corporate and government users had widely adopted Virtual Private Networks (VPNs), which are strongly encrypted. Webmail services such as Gmail and Microsoft’s Hotmail had recently switched to automatically encrypting emails between customers and the email servers. The Snowden revelations have super-charged this shift toward routine encryption of communications. Large gaps had previously existed in where encryption was used in transit; for instance, individual webmail services encrypted between users and servers for their own customers, but routinely sent emails in plaintext when the email passed from one service (such as Gmail) to another (such as Yahoo Mail).[[36]](#footnote-36) These gaps meant that wiretaps often remained possible, in the sense that a wiretap could access plaintext rather than only accessing encrypted zeros and ones. Since the Snowden revelations, however, global communications companies have systematically addressed many of these gaps. They have done so for a number of reasons, including to respond to security flaws highlighted by the Snowden documents, and in order to reassure customers globally that the NSA and other intelligence agencies cannot intercept and read emails and other communications. These security upgrades, in the form of more pervasive use of encryption, mean that law enforcement now often receives no knowledge from a wiretap of Internet communications. When an email goes from Alice to Bob, it is encrypted from Alice to her webmail provider, from that provider to Bob’s email provider, and from Bob’s provider to Bob.

For these emails and other electronic communications, law enforcement thus has a pressing incentive to get the evidence from an email provider, where the communication is generally still in plaintext.[[37]](#footnote-37) Here is where the connection with MLATs becomes so important.

Take the example of a police officer in the United Kingdom, who is investigating a local crime and seeks access to a suspect’s emails. In the old days of telephone calls, the police could wiretap the phone locally. More recently, the police could wiretap emails and other Internet communications locally. Now, with encryption between the suspect and the email provider, no local wiretap is effective – the wiretap only produces indecipherable zeros and ones. The police may find that the suspect uses a webmail service housed in the United States. The only source for the email, then, is for the local police to figure out how to get an MLAT request sent from the U.K. to the U.S., where the webmail provider eventually may be ordered to produce the email. If the MLAT gets an average response time, then the police investigators wait ten months or so after the formal request is made. In a fast-moving criminal investigation, that scale of delay is frustrating to say the least. And note, this example does not assume that the suspect is investigated for a trans-border crime; the same email service might be used by a local co-conspirator. Even for a local crime carried out by local co-conspirators, the emails may be available only internationally, leading to the delays of the MLAT process.[[38]](#footnote-38)

**3. More efficient MLATs can counter the perceived risks of strong encryption.** An additional reason, which deserves more extensive deliberation, is that an effective MLAT process can reduce concerns by law enforcement officials that they are “going dark” due to more pervasive use of encryption technology; efficiently-filled MLAT requests that can access emails and other records in plaintext at the server are an attractive alternative to approaches supported by FBI Director Comey and UK Prime Minister Cameron for weakening encryption technologies.[[39]](#footnote-39)

For the same reason that law enforcement has begun seeking access to the cloud, making that access easier for other justified law enforcement requests would give officials concerned about strong device encryption an alternative means of accessing important data. No matter how well encrypted an individual devices are, true end-to-end encrypted transfers of data are rare. Law enforcement can therefore often access the data in unencrypted format on whatever server or servers the target’s device uses, addressing the need to break the device encryption entirely. Swire has written previously about the risks of weakening encryption and to providing government backdoors, such as concerns about the backdoors being abused or discovered by malicious parties.[[40]](#footnote-40). Indeed, the foundation of Internet commerce relies on strong and trusted encryption, and weakening those standards could pose greater risks to a key commercial infrastructure. If a better, more efficient MLAT process can assuage the concerns of those seeking to weaken encryption standards, then it seems a safer and easier fix than key escrow to address the issues raised by Director Comey, Prime Minister Cameron, and those that share their specific concern.

**B. Challenges Facing Non-U.S. Requests for U.S. Evidence** Technological change is thus driving a large increase in the number and variety of MLAT requests, and the continued spread of encryption in consumer-facing products and services makes the need for trans-border access to evidence even more pressing. We next turn to examining challenges that exist in the current MLAT process, some of which are organizational and others concern the nature of U.S. legal requirements. Although the U.S. itself faces difficulties in receiving evidence through the MLAT process, by far the largest pressure on the current system comes from non-U.S. requests for records held in the U.S., due to the many records held in the U.S. and the relatively strict U.S. legal standards for responding to requests.

Based on our research to date, the overall number of MLAT requests has grown over time, with the largest increase in recent years, not surprisingly, in requests for electronic evidence.[[41]](#footnote-41) According to government officials, electronic evidence requests are the most time- and labor-intensive, so growth in that segment puts disproportionate pressure on the personnel administering MLATs. As discussed in the President’s Review Group Report, the average response time to an electronic evidence MLAT request is approximately ten months. While long, that kind of delay can be handled in a long-term investigation, such as the drug trafficking and money laundering ones involving Swiss banks that led to the first MLAT agreement.[[42]](#footnote-42) However, for everyday law enforcement investigations, a ten month response time is much more difficult. Absent increases in funding for the U.S. MLAT process, and other reforms discussed below, the response time will likely grow, creating even greater dissatisfaction on the part of U.S. allies.

Compounding this issue is the gap between the legal requirements of the US and those of other states, even close allies. Electronic evidence requests served to the US must comply with all US law before being honored, including the search and seizure protections of the Fourth Amendment and the free speech protections of the First Amendment.[[43]](#footnote-43) Even with close allies, the difference between legal standards can vary greatly, making what would be a valid local warrant invalid as part of an MLAT request. For example, in the UK records requests can be issued by administrative public servants. These administrators are analogs to US executive branch officials, part of the governing administration rather than the judicial service. Therefore, an approval from a UK administrator for a warrant request is not facially valid when included in an MLAT request to the US because US law requires warrants to be issued by an impartial magistrate in the judicial branch. Differences in standards for evidence requests compound this problem, and force foreign law enforcement to use different and often more exacting standards in order to comply with US law. For those states whose legal regimes are even more distant from that of the U.S., these problems are even greater, making satisfaction of foreign law enforcement requests even more difficult.

**C. The Effect of MLAT Problems on Localization and Other Internet Governance Issues**

For countries outside of the U.S., the combination of more electronic evidence located abroad (due to encryption and other factors) and high barriers to getting MLAT evidence (due to bureaucratic delays and relatively strict U.S. legal standards) has at least one logical solution – locate the cloud servers in the country that seeks the evidence. With data localization, a country can use its local legal process to gain the electronic evidence, in the short time typical of local criminal investigations and without the friction of meeting the legal requirements of the U.S. or another country. We believe there are compelling arguments against data localization of this sort. We also believe that understanding the MLAT problems, and fixing them, are important precisely to reduce the prevalence of these undesirable data localization initiatives.

President Obama’s NSA Review Group, among others, has made the case against data localization.[[44]](#footnote-44) In general, the United States has a strong interest in promoting an open, interoperable, secure, and reliable information and communication structure. In the debates over Internet governance, to achieve these goals, the U.S. has strongly supported an inclusive multi-stakeholder model of Internet governance. As the Review Group wrote:

A competing model, favored by Russia and a number of other countries, would place Internet governance under the auspices of the United Nations and the International Telecommunications Union (ITU). This model would enhance the influence of governments at the expense of other stakeholders in Internet governance decisions, and it could legitimize greater state control over Internet content and communications. In particular, this model could support greater use of “localization” requirements, such as national laws requiring servers to be physically located within a country or limits on transferring data across borders.[[45]](#footnote-45)

The Snowden revelations have emboldened supporters of localization requirements for Internet communications. Essentially, the distrust of the NSA, U.S. technology companies, and the U.S. government have provided justification to localize information about a country’s residents, to limit the extent to which such data enters the United States. Russia itself has promulgated the most sweeping new localization requirements, which enter into force in 2015.[[46]](#footnote-46) Public debate has suggested a number of possible motives for such localization requirements, including: (1) concern about how records of their citizens will treated in the U.S.; (2) protectionist support for local cloud providers and other information technology companies, with the effect of reducing the market share of U.S. providers; and (3) use of localization proposals as a way to highlight concerns about U.S. intelligence activities, and to create leverage for possible changes in U.S. policy.

In this setting, non-U.S. frustrations with the MLAT process provide an additional, and potentially powerful, argument for localization initiatives. In many countries, the interests of law enforcement and public safety are given a high priority. Where non-U.S. law enforcement officials in fact face significant obstacles to good faith criminal investigations, then they can logically support localization responses. In certain respects, this pro-law-enforcement rationale for localization is stronger than the three other rationales just discussed. First, based on Swire’s experience in the Review Group and elsewhere, any mistreatment of non-U.S. persons in the U.S. intelligence agencies is considerably lower than often alleged in the non-U.S. press. Second, the protectionist rationale for localization is contrary to widely-held norms of international trade, and thus not a legitimate basis for publicly supporting a localization proposal. Third, the actual use of localization proposals as leverage is likely to be limited in practice. By contrast, precisely to the extent that a flawed MLAT process does impede good-faith criminal investigations, then there is an argument, which is more difficult to dismiss, to favor localization initiatives.

Localization laws create a host of negative side effects. The push towards data localization and a splintered Internet infrastructure both weakens the efficacy of the Internet and hinders economic development. The strength of Internet based commerce lies, in part, in the ease of communicating with customers and users worldwide. The Internet’s openness and accessibility has been key to the growth of large players that find a global market, as well as the ability for newer businesses to compete and gain strong user-bases. Data localization laws threaten that model. Start-ups in particular, as well as established businesses, would be forced to weigh the cost of creating and maintaining local data centers against the value of serving that country. In many instances, the costs would vastly outweigh the benefits, meaning that both the companies would lose out on potential revenue and users, and the citizens of that country would be walled off from services and information they would otherwise have. Localization proposals also face the difficulty of how to provide a useful Internet for over 200 nations in the world. Not least, those citizens who rely on foreign servers to engage in political protest and acts of free speech would be cut off from the services they rely on, reducing the Internet freedom values that have become so important for upholding human rights. Creating a series of walled gardens for users based on their country’s ability to convince companies to house data locally would dismantle much of what gives the Internet value.

**D. Conclusion: MLATs as Synecdoche**

As mentioned above, one U.S. official with a literary sensibility has suggested that MLATs are becoming a synecdoche for international Internet cooperation in the wake of Snowden. As just discussed, MLATs and localization proposals are enmeshed in broad issues such as anger at U.S. surveillance practices, protectionist economic impulses, and efforts to bargain with the U.S. to change surveillance practices going forward. Even more broadly, the localization impulse is closely correlated with the United Nations/International Telecommunications Union approach to Internet governance, where each nation plays a more central role in defining how communications and data are handled within that nation. Frustration with the MLAT process feeds into this nation-focused approach to the Internet, counter to the open, interoperable, and international model of communications that the United States has fostered and should favor. Put differently, we should fix the MLAT process to take away a major excuse for a localized and worse Internet.

**IV. Methods for Making the Current MLAT Process Faster, Better, and Cheaper**

This section will explore possible ways to improve the efficiency of the current MLAT process, based on the recommendations issued in the Presidential Review Group on Intelligence and Communication Technologies Report.[[47]](#footnote-47) While Section V will address broader ways to reengineer the MLAT process, methods for improving the current process are vital for two reasons. First, improving the average response time will improve response to legitimate current requests and alleviate some of the pressure and agitation for more troubling workarounds such as forced data localization. Second, alleviating that pressure will allow more time and room to explore and develop broader re-engineering approaches to solve issues of international law enforcement data sharing. These improvements must also balance the desire to streamline the MLAT process with respect for the rule of law, including national sovereignty and the protection of U.S. privacy principles.

The Review Group proposed five ways to improve MLAT efficiency: increase resources to the Department of Justice’s Office of International Affairs (OIA); streamline the number of steps in the total process; create an online MLAT submission form; streamline the provision of records back to the requesting country; and promote the use of MLATs globally and demonstrate the US Government’s commitment to an effective process. These efficiency recommendations were later echoed, and in some cases supplemented, in Woods’ *Data Beyond Borders*, which advocated for many of the same improvements as the Review Group.[[48]](#footnote-48) Ongoing research and engagement with stakeholders will reveal where these efficiency improvements will be greatest, and how to best prioritize the allocation of any new resources. Among these proposals, we stress increasing resources to the OIA and streamlining the process in the U.S. by creation of a “rocket docket” with prosecutors and magistrates who develop expertise in MLAT requests.

1. **Increasing Resources to the Office of International Affairs**

Perhaps the single highest priority for reform is to increase the resources available to the U.S. processing of MLAT requests, primarily through the OIA. The Review Group Report found that, despite a large increase in the number of MLAT requests for electronic communications, funding to the OIA has remained flat or declined over time.[[49]](#footnote-49) While requests for electronic evidence comprise a small number of the total MLAT requests, these requests are a large portion of the recent increase in MLAT Requests. Electronic evidence requests are also the most resource-intensive demands on OIA.[[50]](#footnote-50) Flat or declining budgets in the face of sharply increasing demands has led to the backlog in MLAT requests, with consequent frustration for U.S. allies seeking evidence in the U.S.

The Department of Justice has sought to address the resources problem through increased funding requests for OIA and MLAT processing. For Fiscal Year 2015, the Department of Justice requested a total of $44 million, including an increase of $24.1 million in funding to address MLAT reform, with requests in three categories.[[51]](#footnote-51) First, the largest proposed increases would staff the Criminal Division (primarily OIA) to process MLAT requests as well as provide training and outreach to key foreign partners to help in crafting requests that meet U.S. evidentiary standards.[[52]](#footnote-52) Second, the funding would have provided a dedicated team to support OIA MLAT requests in the District of Columbia and the Northern District of California.[[53]](#footnote-53) Third, the request sought to establish a dedicated Federal Bureau of Investigation (FBI) unit for centralizing and standardizing FBI responsibilities in processing MLAT requests, specifically managing intake, tracking, and management of MLAT requests as well as training to foreign MLAT partners and outreach to ISPs to ensure transparency in the process.[[54]](#footnote-54)

These budget requests are small in comparison with other federal spending activities, but have not yet received approval in Congress. For Fiscal Year 2015, the request passed the House, and seemed to have support in the Senate, but the funding (except for a small amount for the FBI) was ultimately denied. The Administration has proposed similar funding increases for Fiscal Year 2016, and we hope this modest yet important request will be improved. As discussed in Part III, there are compelling reasons to favor a more smoothly operating MLAT system, including: supporting U.S.-based technology companies against protectionist measures that prefer local vendors who do not store records in the United States; reducing the broader risks to Internet governance from data localization proposals abroad; and signaling to European and other allies in the wake of the Snowden revelations of the good faith cooperation of the U.S. with legitimate law enforcement requests from abroad.

Another strong reason to provide improved MLAT funding is to have staffing available to respond to emergencies and other high-profile investigative requests. A prominent recent example concerns the Charlie Hebdo terrorist attacks in France. High-level contacts between the U.S. and France, and rapid response by the holders of evidence, enabled electronic evidence to be procured the same day, despite the normal lag time in the process.[[55]](#footnote-55) Improved funding would enable adequate staffing and the development of regularized methods for high-value investigations, contributing to the reduction in the current tensions between the U.S. and its various MLAT treaty partners. In short, adequate budgets for MLAT activities contributes to better anti-terrorism and other investigations, and meets important public policy and diplomatic goals of the United States.

1. **Streamline the Number of Steps in the MLAT Request Process: Creating an MLAT Rocket Docket**

Along with providing adequate funding, The Review Group Report also noted the delays caused by having multiple persons handle an MLAT request under the current process.[[56]](#footnote-56) We support exploring a variety of measures to streamline the MLAT request process. Notably, we suggest creating a “rocket docket” for handling MLAT requests, which would both process requests expeditiously and clearly signal to stakeholders the priority of processing MLATs promptly and expertly.

Under current procedures, the number of steps to handle an MLAT request is often extensive, with significant delay possible at each step. As Woods has written, the process “requires many hops: from local law enforcement in State A to central government of State A to foreign office of State A to foreign office of State B to central government of State B to local law enforcement of State B.”[[57]](#footnote-57) With our focus on MLAT requests to the United States, it is up to State A to streamline the actual request. The United States, however, can and should streamline the interaction of the central government (OIA) and local law enforcement (U.S. Attorney’s offices). Under current procedures, an OIA lawyer reviews an MLAT request. Once approved, it goes to the office of the U.S. attorney where records are held, and typically lands on the desk of an already-busy assistant U.S. attorney in that district. That attorney, in turn, then seeks an order from the district court, which handles the request as part of its own busy docket. The holder of the records then typically receives the order, sends records to the local U.S. Attorney’s office, who sends it to OIA, who sends it back overseas. To streamline the process, the Review Group recommended having a single office in the U.S. receive and process the MLAT request.[[58]](#footnote-58)

Moving beyond the Review Group recommendation, we now propose creation of a “rocket docket” to handle MLAT requests in the U.S. The term comes from the Eastern District of Virginia, which has an enduring reputation for handling legal cases more quickly than other courts,[[59]](#footnote-59) and has a variety of procedural rules that assist this faster handling of cases.[[60]](#footnote-60) Applied to MLATs, the idea is to have a set of prosecutors and magistrates who work in the same jurisdiction and systematically handle foreign MLAT requests to the United States. Centralizing this function in one district court has a number of advantages. First, combining the separate OIA review and U.S. Attorney work would save a step in the process.[[61]](#footnote-61) Second, the prosecutors assigned to MLATs would be given a clear mission to handle MLATs quickly and well, rather than risk having an MLAT request slip to the bottom of the stack on an Assistant U.S. Attorney’s desk. Third, both the prosecutors and magistrates would develop expertise in MLAT requests, increasing the quality of review and reducing the average time to review each request. Fourth, developing a corpus of MLAT experience in one district would provide greater consistency across applications, including by developing knowledge about the details of law and practice from each requesting country. This knowledge, among other advantages, would extend to knowledge about human rights objections and privacy risks arising from requests in different countries. Fifth, creation of this rocket docket would clearly signal to allies the importance of high-quality and rapid review of MLAT requests, improving transparency and responding to allies’ concerns generally about MLAT procedures.

A statutory change in 2009 appears to make creation of the rocket docket feasible as an administrative matter. In 2009, Congress amended the Electronic Communications Privacy Act to allow any Federal court, without geographical limitation, the ability to issue a warrant under 18 U.S.C. § 2703(d).[[62]](#footnote-62) These 2703(d) orders, as they are called, are the primary means for seeking electronic evidence pursuant to an MLAT request.[[63]](#footnote-63) In effect, this amendment to ECPA has permitted one district court, its prosecutors, and its local magistrate judges to handle all or the bulk of MLAT requests, effectively allowing for specialization in assessing and carrying out these requests.

The DOJ’s budget request would help to create this specialty capability. The request would assign dedicated US Attorneys, both in DC and Northern California, to assist with MLAT requests. Establishing the rocket docket in the District of the District of Columbia quite possibly is the best choice due to the location of OIA. On the other hand, there are advantages to concentrating personnel in the locations of the technology companies most likely to receive 2703(d) orders. Additional research with stakeholders can clarify the best way to organize this sort of streamlined system. Establishing some version of a rocket docket will reduce the need for multiple hand-offs and lag time as unfamiliar parties are brought up to speed on how to handle the MLAT process.

1. **Streamline Provision of the Requested Records Back to the Requesting Country**

The Review Group Report noted that, under the current process, providers of requested information send it to the Department of Justice, which then forwards the records on to the requesting country.[[64]](#footnote-64) Similar to creating a single point of contact between the requesting country and the record holder, allowing for a direct response to the requesting country would reduce the overall response time. To date, no proposals have been made to allow for direct response to MLAT requests once they are cleared by US Attorneys and OIA.

One method for creating a direct response to requests could be built off of an online submission process. Cleared requests could give the record holders access to the system, allowing them to submit responsive documents directly through the server. Since an individual request would be linked to both the assigned attorney and the point of contact at the requesting country, an electronic submission could be given directly to the requester while also allowing OIA to review the responsive document as well.

1. **Other Steps to Increase Efficiency of the MLAT Process and Demonstrate the U.S. Government’s Commitment to Effective Practices**

The Review Group and Woods’ Reports contain a number of similar efforts to improve the efficiency of the MLAT process and to demonstrate the U.S. government’s commitment to effective practices.

More effective online information about MLATs and online methods to make MLAT requests are natural parts of updating the MLAT process. Today, MLAT requests are still submitted in physical form, without a standardized template or form. The Review Group Report recommended using an online submission form as a way to both improve the efficiency of the request transmission and enable baked-in electronic tracking and organization capabilities.[[65]](#footnote-65) Woods makes similar and additional proposals for online and standardized submissions, and he emphasizes the role that these online materials can play in educating law enforcement officials and others involved in the process. Part of the OIA’s budget increase request includes personnel and funding for training and outreach to foreign governments to assist in understanding US legal standards pertinent to MLAT requests. Such government efforts might be supplemented by private stakeholder efforts to provide accessible, high-quality information about the MLAT process as well as forms for lawful requests.

There may be other ways to reduce the number of steps in the process. The Review Group Report noted that records holders currently respond to requests by sending records to the Department of Justice, which then forwards the records to the requesting country.[[66]](#footnote-66) Similar to creating a single point of contact between the requesting country and the record holder, allowing for a direct response to the requesting country would reduce the overall response time. Additional work by stakeholders might identify whether, and with what safeguards, this sort of direct provision to the requesting country may be appropriate.

Lastly, the Review Group Report suggests that the US government publicize and support an improved and functioning MLAT process in order to support the continued global use of efficient and innovation internet technologies.[[67]](#footnote-67) Effective public relations around an improving and important MLAT process would be an effective way of advocating on behalf of US-based internet companies that encrypt their web traffic. Making sure that other countries know the MLAT process is a priority and is working more efficiently will likely make those governments less likely to seek other ways to force ways to make up for their inability to conduct wiretaps on internet communications, such as data localization requirements.

The Review Group report emphasized that changing technology has sharply increased the importance for non-US governments of gaining lawful access to records held in the United States.[[68]](#footnote-68) Web e-mail providers are largely headquartered in the United States, and today’s use of secure encryption for e-mail means that other governments frequently cannot intercept and read the e-mail between the user and the server. It is in the interest of the United States to support the continued use of efficient and innovative technologies on the Internet, including through leading web e-mail providers. The US Government can promote this interest by publicizing and supporting the existence of a well-functioning MLAT process, thereby reducing the likelihood of harmful localization measures.

One other means of underscoring the US’s commitment to an improved MLAT process is to make company transparency reports able to reflect the difference between MLAT-based government data requests and other requests. Woods noted that companies receive MLAT requests as a local warrant for data, often without any indication of which country is requesting the information.[[69]](#footnote-69) Woods suggests that allowing companies to identify and report which countries are requesting and receiving data through MLATs would improve the accuracy of corporate transparency reports, and that countries should embrace similar reporting methods as a means of helping policymakers improve MLAT efficiency.[[70]](#footnote-70) This kind of reporting, both on the corporate and government levels, would also effectively highlight improvements to the MLAT process. By showing the number of requests by country, along with when those requests were fulfilled, the U.S. government would have another means of demonstrating its commitment to enabling access to US-based data for foreign countries engaged in lawful investigations.

These changes as a whole would serve to greatly improve the efficiency and response time for current MLAT requests, as well as relieving some of the building international pressure to give foreign law enforcement direct access to web e-mail and other data that is often stored in the cloud. These efforts to make the MLAT process faster, better, and cheaper are essential, but they are not enough to turn a ten-month average turnaround time into a ten-hour one. However, making the current process better, faster, and cheaper will likely not be enough to turn an average of a 10-month turnaround time into a 10-hour one. Broader re-engineering of the MLAT process is also needed.

**V. Re-Engineering the MLAT Process**

This Part proposes two analogies for re-engineering the MLAT process over the longer term. The first is the Visa Waiver Program, so that qualifying countries could have a streamlined way to have their MLAT requests handled in the U.S. The second scales the use of joint criminal investigations, with the analogy to an online dating service.

**A. A Streamlined MLAT Program Similar to the Visa Waiver Program**

What we will call the “streamlined MLAT” program is conceptually similar to the Visa Waiver Program (VWP), administered by the Bureau of Consular Affairs of the U.S. State Department.[[71]](#footnote-71) As a general rule, foreign visitors to the United States must receive a visa individually issued by the State Department. As globalization increased the number of international travelers, individual interviews for visas became more difficult to manage. Since 1986, citizens of eligible countries face a greatly streamlined process in visiting the U.S. for short visits of up to 90 days. The detailed requirements for an individual visa are waived. Applied in the MLAT context, due to the analogous globalization in cross-border evidence, the idea is that eligible countries, with high-quality procedures for seeking evidence, would face a streamlined process for gaining evidence in the U.S.

In this discussion, we make the analogy to the Visa Waiver Program, and show reasons why specific aspects of that program are useful precedents for a streamlined MLAT program. We also examine how the streamlined MLAT program would be assessed under the Electronic Communications Privacy Act and the Fourth Amendment, showing reasons to believe a well-crafted program would be constitutional and practical, and identifying areas for additional research and deliberation.

**1. The analogy to the Visa Waiver Program.** The existing VWP provides a very helpful model for the issues that a streamlined MLAT program would face. We suggest possible approaches to these issues, and then assess the overall desirability and workability of the visa waiver approach to MLATs.

For the VWP, countries can become eligible if the history of their visa applications demonstrates high quality, measured by a low nonimmigrant visa refusal rate.[[72]](#footnote-72) The statute provides a list of other requirements for a country to be eligible, including that the country: issues machine-readable passports; has an agreement with the U.S. to report lost and stolen passports; promptly accepts its citizens for repatriation if there is a U.S. order of removal; and has an agreement with the U.S. for passenger information exchange.[[73]](#footnote-73) The Secretary of Homeland Security, after consultation with the State Department, must certify that the visa waiver is in the national interest. The statute requires the Secretary to evaluate the effect that the countries’ designation would have on the law enforcement and security interests of the United States, determine that such interests would not be compromised by designation; and submit a written report to Congress about the findings.[[74]](#footnote-74)

For a student of the MLAT debate, the detailed provisions for the VWP are instructive. The VWP statute sets forth criteria for what counts as a high-quality foreign partner. One can easily imagine developing criteria for what counts as a high-quality MLAT request to the U.S., although this paper will not attempt to propose detailed provisions.[[75]](#footnote-75) The VWP includes a technological requirement to reduce fraud – a machine-readable passport – and technological requirements such as strong authentication of the requesting party might be included in an MLAT version. The VWP requires that the other country enter into supplementary agreements, such as the repatriation and passenger information agreements. For MLATs, one can imagine also requiring supplementary agreements that fill in details about the two countries will cooperate. For instance, a condition of the U.S. providing streamlined MLAT treatment might be that the other country provides streamlined procedures for U.S. requests.[[76]](#footnote-76) As for procedure, it seems plausible that the Attorney General would make the certification decision about foreign legal procedures, after consultation for diplomatic insights from the State Department.

**2. Assessing the analogy to the Visa Waiver Program.**  The similarities of the VWP and the streamlined MLAT program are striking. For visas, the growing tide of foreign travel placed increasing pressure on the U.S. government gatekeepers – the consular officials – to decide when official U.S. government permission should be granted. Similarly, for MLATs, the growing tide of foreign evidence requests is placing increasing pressure on the U.S. government gatekeepers – the Office of International Affairs in the Department of Justice – to decide when official U.S. government permission should be granted. For visas, the solution was to treat different countries differently. For countries with the highest-quality visa applications, the U.S. government, after thorough review for the national interest, provided a streamlined process. For MLATs, the proposal would be to provide a similarly streamlined process for high-quality evidence requests. Along with other reasons for supporting the change, U.S. economic interests are at stake. For the VWP, the streamlined procedures helped U.S. tourism as well as business visits to the U.S. that could spur exports. For MLATs, the streamlined procedures, among other effects, would reduce the frustration of U.S. allies, reduce the incentives for localization laws in other countries, and help technology companies based in the U.S. to operate overseas without constant criticism based on the current MLAT process.

The historically gradual adoption of the VWP would likely apply to any streamlined MLAT program. The VWP began slowly. After the 1986 law creating the program, the United Kingdom and Japan joined the program in 1988, followed by France, Italy, the Netherlands, Sweden, Switzerland, and West Germany the following year. As of early 2015, 38 countries are eligible for the VWP,[[77]](#footnote-77) with others under consideration that has lasted for multiple years.[[78]](#footnote-78) For MLATs, a streamlined program would likely also take some number of years to develop. So far as we can determine, the program would require U.S. legislation.[[79]](#footnote-79) If and when a statute passes, meeting the requirements for eligibility may take additional years, as was the case for the VWP. The program would likely take effect first with a handful of close allies, and only gradually expand over time. This lengthy timeline suggests that a streamlined MLAT program may be a worthy long-term goal to address global evidence requests, but that the efficiency and other proposals would be important to pursue in the interim.

**3. The Fourth Amendment and related issues.** This article sets forth the idea of a streamlined MLAT program. Assessment of the constitutionality of a particular such program would depend on its details, so the discussion here sets forth key concepts, as well as reasons to believe that a well-crafted program would pass constitutional muster.

The basic legal structure we propose is a new statute to create the streamlined MLAT program, setting forth criteria for procedures in other countries that would support a finding by the Attorney General that a country qualifies for a waiver of the usual MLAT requirements. An important consideration in drafting the statute is how it would interact with existing or possible future requirements of the Electronic Communications Privacy Act. Our research indicates that ECPA has relatively strict requirements compared to most other legal systems, especially concerning the role of a federal judge in deciding whether to issue a 2703(d), search warrant, or other order. For instance, the United Kingdom, with its similar legal traditions to the United States, would presumably be an early candidate for an MLAT waiver. Yet the U.K. authorizes government access to email and other electronic records primarily by administrative officials rather than requiring a judicial order.[[80]](#footnote-80) Proposals for a streamlined MLAT program would thus need to consider how to assess when the non-U.S. procedures are adequate, even when they are not identical or equivalent to U.S. procedures.[[81]](#footnote-81) The tension between U.S. and foreign regimes could become more acute if ECPA is amended to raise the standard for government access to e-mails and other electronic evidence, as has been prominently supported by consumer groups, technology companies, and other members of the Digital Due Process Coalition.[[82]](#footnote-82) We are sympathetic to the Coalition’s efforts, but write here to propose further study about the intersection of MLAT reform and the Coalition’s proposals.

Whatever the statutory intersection with ECPA, the streamlined MLAT program would of course have to be consistent with the Fourth Amendment’s requirements about searches and seizures. Under the approach favored by the U.S. Department of Justice, the program would presumably be constitutional because the electronic records are held by third parties such as email providers. Following cases such as *Smith vs. Maryland*,[[83]](#footnote-83) the Justice Department has continued to argue that users have no reasonable expectation of privacy in the content of their emails. The Sixth Circuit, in *U.S. v. Warshak*, held otherwise, finding that there is a reasonable expectation of privacy in the content of e-mails stored on third party servers, triggering a Fourth Amendment requirement of a search warrant for the government to access those e-mails.[[84]](#footnote-84) Justice Sotomayor, in *U.S. v. Jones*, wrote: “More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.”[[85]](#footnote-85) A growing literature by professors and others has been exploring ways to amend or discard the third-party doctrine, and replace it with some different Fourth Amendment approach.[[86]](#footnote-86)

In this article, we do not take a position about whether or how the third party doctrine might change over time. If the courts follow in the direction of *Warshak* and Justice Sotomayor’s opinion, then we may see more holdings that a probable cause search warrant will be required in a range of circumstances. With that said, there is a different basis for meeting Fourth Amendment requirements, based on what counts as an “unreasonable” search or seizure. Our view at this time is that requests from a nation with high-quality legal procedures might quality as “reasonable” even if not founded on a probable cause search warrant in the foreign country. One prominent example of this reasonableness approach comes from In re Sealed Case No. 02-001, a per curiam decision by the U.S. Foreign Intelligence Surveillance Court of Review.[[87]](#footnote-87) That case assessed 2001 USA PATRIOT Act changes to FISA to broaden how easily evidence gathered for foreign intelligence purposes could be used for criminal prosecution. The court addressed the issue of whether “government surveillance whose primary purpose is criminal prosecution of whatever kind is per se unreasonable if not based on a warrant.” The court found that the Fourth Amendment did not require a probable cause warrant in the foreign intelligence context examined by the court. The court did a more holistic assessment of multiple features of the overall regime, finding it “reasonable” and thus consistent with the Fourth Amendment.

This reasonableness assessment of foreign intelligence requests for records is suggestive of how courts might assess the reasonableness of an evidence request from a country that the Attorney General has certified meets the standards in an MLAT-waiver setting. In our era of pervasively global communications flows, it would be somewhat arrogant to take the position that only a U.S.-style probable cause warrant is “reasonable” when seeking electronic evidence across borders. Many other countries besides the United States have effective democracies and rule of law, including concerning the gathering of electronic evidence. The Visa Waiver Program has demonstrated the possibility of U.S. law meshing effectively with the laws and practices of other countries to address globalization issues, and a similar approach is promising for global electronic flows.

As an additional area for further research, it is possible that a streamlined MLAT program could apply differently to evidence about U.S. persons and non-U.S. persons. MLAT requests going forward are likely increasingly to involve foreign requests for communications between non-U.S. persons, with the storage of the evidence happening to be in the United States. For instance, a German investigation might involve emails between a German and a French citizen, and the policy interest in applying U.S. standards to such requests is arguably less than for communications that are to or from a U.S. address or involve U.S. citizens. An analogous issue arose during the amendments to FISA in 2007 and 2008. The question there was how much to apply U.S. wiretap law to communications that “transited” the U.S., such as from Europe to Asia, but that were accessed inside the U.S. and had at least one end point outside of the U.S. In the FISA Amendments Act of 2008, Congress addressed this issue in Section 702.[[88]](#footnote-88) Essentially, Section 702 allows access to communications within the U.S. with a lower standard if various conditions are met, notably that at least one end of the communication is outside of the U.S. and the investigation is not targeted at a U.S. person. The analogy to MLATs is worth exploring – since less restrictive standards apply to electronic communications governed by Section 702, similarly less restrictive standards might apply (as a matter of policy or constitutional law) to e-mails and other stored communications that simply “transit” the U.S. but where the investigation is not targeted at a U.S. person.

In sum, this article puts forward the promising analogy of the Visa Waiver Program as a way to re-engineer a legal regime that is placed under pressure by globalization. We outline the possible structure of a streamlined MLAT process, and suggest areas for further research and deliberation.

**B. Scaling the Use of Joint Criminal Investigations – the Online Dating Service Analogy**

One of the easiest ways to avoid the procedural hurdles of traditional MLAT requests is to conduct a joint investigation. As a general matter, law enforcement in two different countries can share information as part of investigating the same crime.[[89]](#footnote-89) For example, suppose that German law enforcement is investigating an online computer crime organization, and German police wish to access webmail or other records housed on servers in the United States. The traditional MLAT approach would be for the German police to use their national procedures to send a request to the U.S. Department of Justice. The request would go into the current backlog in the U.S., perhaps taking ten months before a response is provided, even where sufficient evidence exists to meet U.S. legal requirements. By contrast, a joint investigation could proceed much more quickly. If the German police and the FBI are investigating the same crime, the FBI and the U.S. Department of Justice could use the standard domestic procedures to seek the records in the U.S. Those procedures, on average, are much faster than MLATs. Based on the interviews we have conducted, non-emergency webmail and other requests of this sort are often fulfilled in a week or two.[[90]](#footnote-90)

The advantages of using joint investigations are known to police working on cybercrime and other cases that have a significant cross-border component. The U.S. and other countries have conducted training sessions that bring police from multiple countries together, with one positive feature of the training to create person-to-person connections that can facilitate joint investigations in the future.[[91]](#footnote-91) For instance, after such joint training, a German police officer might contact an FBI agent who was in the same training session, asking for assistance and the opening of a joint investigation to target the computer crime organization.

Although the possibility of joint investigations is thus known within law enforcement, we are not aware of previous discussion about scaling the use of joint investigations into a major solution for today’s MLAT challenges. With apologies if the analogy sounds not serious enough, our proposal is to create the equivalent of an online dating service for joint investigations. Consider how the online dating service could work: an investigator in one country learns about evidence in a second country that is relevant to the criminal investigation. The investigator goes to the dating service website, and fills out a form explaining what sort of evidence is needed in what country. Then, a law enforcement official in the second country could review the request. If the date seems attractive (more in a moment about what would make it attractive), then the official in the second country could reply. As with a dating service, the two parties with similar interests might find each other extremely quickly, in hours or a few days. When there is a successful match, the evidence would be gathered under the domestic rules of the second country and then shared to the first country, on a domestic law enforcement time line (days or a few weeks) rather than an MLAT time line (many months).

The central idea is thus to address the MLAT problem of cross-border access to evidence with the conceptual model of an online dating service – remote matching of individuals and organizations in the requesting and the receiving countries. Although many details would need to be worked out to build the dating service, we begin consideration of the approach by discussing four key considerations, while encouraging broader discussion of whether and how to construct that service. These initial considerations are: using an Internet solution to an Internet problem; the need for little or no legislative or treaty change; financial considerations; and issues about the institutional structure of the dating service, including maintaining confidentiality of investigative data.

**1. An Internet solution to an Internet problem.** This paper has emphasized how the development and growth of the Internet have created enormous pressure on the traditional MLAT system, for at least three inter-related reasons. First, the Internet facilitates cross-border conspiracy and other activity by reducing communications costs. Second, the importance of evidence held in other jurisdictions has risen even more sharply because of the prevalence of information relevant to the requesting country’s investigation being held in the receiving country. Third, the recent predominance of encrypted communications means that email and voice wiretaps in the requesting country are increasingly rendered useless, so investigators can only get plaintext evidence from the receiving country.

One great advantage of the online dating service approach is that it employs an Internet solution to this Internet problem. Before the Internet, communication between police in two countries was typically costly and slow, via mail or expensive international phone calls. Today, police gain the same advantages as criminals of instant and essentially free global communications. The online dating service matches individuals in the requesting and receiving countries,[[92]](#footnote-92) including for police departments who previously would not have known whom to contact in the receiving country. This matching function is similar to Airbnb, which encourages consumers to “Rent unique places to stay from local hosts in 190+ countries.”[[93]](#footnote-93) It is also analogous to Internet-based taxi service Uber, which as of April, 2015 reports “56 Countries: Available locally, expanding globally.”[[94]](#footnote-94)

The idea of the online dating service opens up the possibility of online matching of whichever countries have requests for evidence in whatever country. Negotiating and implementing MLATs has historically been a slow and arduous process, often including long delays until two particular countries resolve how requests from one legal system can be accommodated in the receiving legal system.[[95]](#footnote-95) The online dating service approach replaces the laborious, bilateral MLAT approach with an Internet-based process that is designed to add new participants in ways analogous to new participants in the dating service, Airbnb, or Uber.

**2. The need for little or no legislative or treaty change to improve MLAT-type requests.** To date, discussions about change in MLAT procedures have confronted two high institutional obstacles. First, it is a difficult and slow process to amend each MLAT treaty, and the sheer number of existing bilateral treaties makes systematic reform difficult to contemplate. Second, many possible reforms to MLATs would require legislative change in one or more countries. To take a simple example, it would be far simpler for the U.S. to respond to MLAT requests if the U.S. decided to repeal the procedural safeguards in the Electronic Communications Privacy Act. Enacting any changes to ECPA, however, is extremely difficult. To the extent there has been recent momentum for reform, moreover, it has been in the direction of strengthening privacy protections, such as in proposals of the Digital Due Process Coalition. That coalition is actively pushing for legislation whose first reform is to confirm that a search warrant rather than a subpoena should be required for government access to emails and other information stored online: “The government should obtain a search warrant based on probable cause before it can compel a service provider to disclose a user’s private communications or documents stored online.”[[96]](#footnote-96)

To achieve MLAT reform, therefore, it is enormously helpful to identify measures that can be instituted without modification of treaties or new legislation. The online dating service, so far as we can determine, can be instituted for many countries without the need for treaty or legislative change. Joint investigations are generally permitted today where there is “dual criminality” – where the activity being investigated is a crime in both countries. The Budapest Convention, also known as the Council of Europe Cyber-Crime Convention, specifically addressed the issue of dual criminality for a wide range of cyber-related crimes and investigations. In addition to the Council of Europe members, the Convention has been ratified by the United States, Japan, Australia, and other countries.[[97]](#footnote-97) Moreover, beyond countries that have ratified the Budapest Convention, a wide range of conduct is criminal under the laws of numerous countries, including narcotics, money laundering, child exploitation, and other crimes that often have an international dimension in the criminal conduct. Moreover, much of this criminal activity will include use of computing resources in the receiving country and evidence of a conspiracy that takes place at least in part in the receiving country.[[98]](#footnote-98) Where dual criminality does not already exist, moreover, any particular requesting or receiving country could consider amendments to its own criminal law to enable it to participate in the online dating service for that category of criminal conduct.

**3. Financial considerations.** Misaligned incentives plague requests for evidence from distant jurisdictions. Essentially, the case is a high enough priority in the requesting jurisdiction to justify scarce investigative resources. For the receiving party, however, the request generally does not have the same priority – even where evidence exists in the receiving jurisdiction, the criminals are usually elsewhere. The receiving jurisdiction would prefer to spend its time protecting its local citizens rather than citizens from another country.[[99]](#footnote-99)

Although these misaligned incentives are potentially a major obstacle to the dating service approach, we suggest a number of possible solutions. First comes methods familiar in the dating world relying on reciprocity and personal relationships, so that investigators in the receiving country are willing to assist the requesting country. Second is the rocket docket approach discussed in Part IV. For the U.S., a dedicated office with sufficient resources can and should exist in Washington, D.C. to staff incoming requests. Because effective MLAT-style procedures are a benefit to the United States and its foreign policy, federal funding is appropriate to meet these federal goals. The scale of funding would also appear manageable, overlapping with and similar in scale to the modest funding requested for the Office of International Affairs.

A third funding approach is a bit more creative but may prove useful in a range of countries. In the U.S. and other countries, law enforcement has long paid for wiretaps and other access to evidence where there is a significant cost to the companies holding the records.[[100]](#footnote-100) This wiretap funding is directly relevant to the increase in cross-border requests. As discussed in Part III, the increasing use of encryption has reduced the effectiveness of local wiretaps in many instances. We can think of the funding for wiretaps going instead to requests through the dating service; after all, the traditional investigation that used a wiretap instead now seeks access to a webmail server in another country, and so it is reasonable to ask the requesting investigators to pay costs incurred by others. Existing budget lines for wiretaps would instead go to a slightly broader range of uses, including the cost of accessing evidence through the dating service. A related, fourth, approach would be for the largest countries in the dating service to cover the operating expenses. In many systems, a small fraction of the participants conduct a large fraction of the activity. This is colloquially known as the “80/20 Rule,” such as where 80 percent of the business comes from 20 percent of the customers.[[101]](#footnote-101) The suggestion is that the countries most engaged in the online dating service (the 20 percent) could pay all or almost all of the operating expenses. That could simplify management and funding of the dating service. In more academic parlance, we are suggesting the approach that Mancur Olson called “the exploitation of the great by the small.”[[102]](#footnote-102) In essence, the biggest players (including the U.S.) have a large enough stake in the system that they can afford to cover some or all of the costs of the smaller players.[[103]](#footnote-103)

**4. Institutional considerations, including confidentiality.** The goal in this discussion is to introduce the concept of greatly scaling up joint investigations across borders, using the analogy of an online dating service to match requesting and receiving jurisdictions. One might imagine a variety of institutional structures for implementing the dating service. Existing arrangements through Interpol or other existing organizations might be modified to support the dating service. Instead, to more nimbly address the particular current problems related to MLATs, the U.S. and allies might create a new organization focused on the speedy and high-volume response to the growing number of requests, especially for emails and other electronic evidence. The next phase of MLAT reform could consider what institutional structure could work best.

The new institution would need to address a variety of operating issues, notably relating to cybersecurity and privacy. The dating service would need to create an authentication system, to enable access by qualified law enforcement officials but screen out interlopers. Confidentiality procedures are also important, to protect the investigation as well as the privacy of the individuals whose information is included in the evidence sought for cross-border transfer.

Here is one place where the analogy to an online dating service is especially apt. Participants on dating sites initially post only highly edited information about themselves. Once a relationship begins to develop, and some degree of trust is established, the participants are willing to disclose more sensitive and personal information. Similar initial caution is appropriate for an investigative request that flows in from a distant country; after background checks and a first date, the person receiving the request can decide whether and how to move forward with the relationship.

The online dating service also provides protection against low-quality requests from abroad. Suppose that a request arrives from a country that lacks strong legal due process protections, perhaps requesting evidence about behavior that is protected by the First Amendment in the U.S. For this low-quality request, the U.S. investigators would refuse the invitation for a date – they would not open a joint investigation.

Analogies to the dating service aside, a promising path for MLAT reform is to explore more systematic and scalable ways to conduct joint investigations. Stakeholders should explore where and how such joint investigations would prove fruitful, as well as situations where there are legal, financial, or other obstacles to use of joint investigations.

**VI. Conclusion**

When MLATs were first introduced they addressed the problems of investigating well-organized international criminal conspiracies. Money launderers and drug traffickers were no longer able to hide confidently in Swiss banks, knowing that crimes in America were not enough to get the police access to Swiss financial records. Unfortunately, the advent of the Internet and encrypted communications have drastically increased the pressure, and MLATs are no longer the solution they once were. We see evidence of this in cracks forming through the push for data localization and weakened or back-doored encryption standards. MLATs are still the best means for alleviating the pressure, but need to be re-engineered to do so effectively.

The first step is to increase the efficiency of the current process. Doing so will both demonstrate a continued commitment from the U.S. and make the process itself faster for foreign law enforcement, thereby alleviating the need to find other ways to access data. Better efficiency also gives more time for step two: re-engineered MLATs. This paper has proposed two models for changing the way law enforcement accesses data: the online dating service model, and the visa-waiver model. Each of these processes have the potential to create a more transparent and efficient system of response for data requests, and can continue to scale as the number of requests grows, while maintaining protection for privacy and free speech.

The next step is to convene stakeholders in the MLAT process to discuss these re-engineering solutions, and make progress. Further research should be conducted on the increasing scale and types of requests, and how different models may be able to better address them. Stakeholders would also see demonstrated movement on improving the process, while making strides toward agreements and even pilot programs around these ideas. Some progress, however, must be made if MLATs are to remain a primary means of providing trans-border access to data for law enforcement.

1. \* Peter Swire is the Huang Professor of Law and Ethics at the Georgia Institute of Technology’s Scheller College of Business, and Senior Counsel, Alston & Bird LLP. This draft paper is prepared for the NYU School of Law Symposium on Government Access to Data in the Cloud and the Privacy Law Scholars Conference ’15. Our thanks for research funding from the Future of Privacy Forum, the Georgia Tech Information Security Center, the Georgia Institute of Technology’s Scheller College of Business, and Microsoft Corp. [↑](#footnote-ref-1)
2. \*\* Justin Hemmings is a Research Associate at the Georgia Institute of Technology’s Scheller College of Business and a Policy Advisor at Alston & Bird, LLP. He received his J.D. from American University’s Washington College of Law. [↑](#footnote-ref-2)
3. *See* T. Markus Funk, *Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges*, Federal Judicial Center International Litigation Guide (2014). [↑](#footnote-ref-3)
4. U.S. Department of State, “Preparation of Letters Rogatory,” *available at* http://travel.state.gov/content/travel/english/legal-considerations/judicial/obtaining-evidence/preparation-letters-rogatory.html. [↑](#footnote-ref-4)
5. *Id.* [↑](#footnote-ref-5)
6. *Id.* [↑](#footnote-ref-6)
7. *Id.* [↑](#footnote-ref-7)
8. *See* Paul R. Dubinsky, *Is Transnational Litigation a Distinct Field? The Persistence of Exceptionalism in American Procedural Law*, 44 Stan. J. Int’l L. 301, 335 (2008). [↑](#footnote-ref-8)
9. *See* Unif. Interstate Depositions and Discoveries Act prefatory note (2007) *available at* http://www.uniformlaws.org/shared/docs/interstate%20depositions%20and%20discovery/uidda\_final\_07.pdf. [↑](#footnote-ref-9)
10. *See id.* [↑](#footnote-ref-10)
11. *See* Robin H. Jones, *Can I Get A Witness: Obtaining Out-of-State Deposition Subpoenas*, Ala. Lawyer, 472 (Nov. 2011). [↑](#footnote-ref-11)
12. *See id.* [↑](#footnote-ref-12)
13. *See id.*; *see also* UIDDA. [↑](#footnote-ref-13)
14. *See id.* [↑](#footnote-ref-14)
15. Fed. R. Civ. P. 45 [↑](#footnote-ref-15)
16. UIDDA. [↑](#footnote-ref-16)
17. Tex. R. Civ. P. 201.1(c), 201.2 [↑](#footnote-ref-17)
18. *See* *U.S. Practice: Contemporary Practice of the United States Relating to International law*, 86 A.J.I.L. 548 (Jul. 1992). [↑](#footnote-ref-18)
19. *See 28 U.S.C. § 1782 as a Means of Obtaining Discovery in Aid of International Commercial Arbitration – Applicability and Best Practices*, 63 The Record 752, 753-54 (2008) (noting that the Act, and its subsequent supplemental “Act to facilitate the taking of depositions within the United States, to be used in the Courts of Other Countries, and for other purposes,” were passed in response to a previous U.S. Attorney General’s opinion that U.S. courts lacked the statutory authority to respond to execute a French court’s letter rogatory). [↑](#footnote-ref-19)
20. *See id.* at 754. [↑](#footnote-ref-20)
21. *See* William W. Park, *Symposium: Scholarship in Banking Law: Legal Policy Conflicts in International Banking*, 50 Ohio St. L.J. 1067, 1097 (1989). [↑](#footnote-ref-21)
22. *See id.* [↑](#footnote-ref-22)
23. *See* 2012 Int’l Narcotics Control Strategy Rep., *available at* http://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm. [↑](#footnote-ref-23)
24. *See* Inter-American Convention on Mutual Assistance in Criminal Matters (“The states parties shall render to one another mutual assistance in investigations, prosecutions, and proceedings that pertain to crimes over which the requesting state has jurisdiction at the time the assistance is requested”) *available at*  https://www.oas.org/juridico/english/Treaties/a-55.html. [↑](#footnote-ref-24)
25. T. Markus Funk, *Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges*, Federal Judicial Center International Litigation Guide (2014). [↑](#footnote-ref-25)
26. *Id.* [↑](#footnote-ref-26)
27. Rep. and Recommendations of The President’s Review Group on Intelligence and Communications Technologies (Dec. 12, 2013) *available at* https://www.whitehouse.gov/sites/default/files/docs/2013-12-12\_rg\_final\_report.pdf. [↑](#footnote-ref-27)
28. Andrew K. Woods, *Data Beyond Borders Mutual Legal Assistance Treaties in the Internet Age*, Global Network Initiative 6-7 (Jan. 2015). [↑](#footnote-ref-28)
29. In our interview, the official gave us permission to use this term, but not to cite the official by name. [↑](#footnote-ref-29)
30. In the mid-2000s, Swire served as an advisor to an anti-spam company called Blue Security, which eventually closed down after confrontations with non-U.S. based spam rings. *See* Brian Krebs, *In the Fight Against Spam E-Mail, Goliath Wins Again*, Wash. Post., May 17, 2006, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/05/16/AR2006051601873.html. [↑](#footnote-ref-30)
31. Peter Swire, *From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud*, 2 Int’l Data Privacy Law 200 (Nov. 2012) *available at* http://idpl.oxfordjournals.org/content/2/4/200. [↑](#footnote-ref-31)
32. 47 U.S.C. § 1001-20 (2012). [↑](#footnote-ref-32)
33. The official press release for the Order is available at http://hraunfoss.fcc.gov/edocs\_public/attachmatch/DOC-260434A1.pdf. [↑](#footnote-ref-33)
34. See panel discussion of “Why Traditional Encryption Products Have Low Adoption,” available at https://www.voltage.com/PKC/index.htm. [↑](#footnote-ref-34)
35. Swire, at 4. [↑](#footnote-ref-35)
36. *See* Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 360 J. on Telecomm. & High Tech. L. 359 (2010). [↑](#footnote-ref-36)
37. This strategy does not work if the customers use end-to-end encryption, where even the email server sees only encrypted text. The market penetration for end-to-end email encryption, however, remains very low at the time of this writing. Email becomes less convenient for many users with end-to-end encryption, including the risk that the user will lose the keys and thus all access to emails will be loss. Email providers also have business reasons to prefer having access to plaintext at the server, including to enhance features and provide advertisements.

    Another law enforcement strategy is to access plaintext from either Alice or Bob, such as by gaining access to their smartphones or other devices. This issue has been the subject of intense public debate since FBI Director Comey in the fall of 2014 criticized Apple and Google for deciding not to have a master key for access to smartphones. *See* Craig Timberg & Greg Miller, *FBI Blasts Apple, Google for Locking Police Out of Phones*, Wash. Post, Sep. 25, 2014, *available at* http://www.washingtonpost.com/business/technology/2014/09/25/68c4e08e-4344-11e4-9a15-137aa0153527\_story.html*.* The debate about device encryption is generally outside the scope of this article, except to note that law enforcement access to evidence in the cloud (and therefore the MLAT process) becomes even more important if law enforcement cannot access plaintext at either the device or in transit. [↑](#footnote-ref-37)
38. In practice, the police may use a wide variety of traditional law enforcement techniques other than access to e-mail, such as physical search of a suspect’s residence, seeking to turn one member of the conspiracy, and so on. The point here is not that the investigation is necessarily stopped in its tracks. Instead, the point is to emphasize the frustration of a police investigator who can no longer get a useful wiretap and has to wait to see if evidence will be produced from abroad. [↑](#footnote-ref-38)
39. (cite) [↑](#footnote-ref-39)
40. Peter Swire & Kenesa Ahmad, “Encryption and Globalization,” 13 *Colum. Sci. & Tech. L. Rev.* 416(2012). [↑](#footnote-ref-40)
41. [These facts are based on interviews to date with officials, and we are seeking the ability to report in more detail in later versions of this paper.] [↑](#footnote-ref-41)
42. Alan J. Kreczko, *U.S. Practice: Contemporary Practice of the United States Relating to International Law*, 86 A.J..I.L. 548 (1992). [↑](#footnote-ref-42)
43. T. Markus Funk, *Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges*, Federal Judicial Center International Litigation Guide (2014). [↑](#footnote-ref-43)
44. Rep. and Recommendations of The President’s Review Group on Intelligence and Communications Technologies at 214-16 (Dec. 12, 2013) *available at* https://www.whitehouse.gov/sites/default/files/docs/2013-12-12\_rg\_final\_report.pdf. [↑](#footnote-ref-44)
45. Id. at 214-15. [↑](#footnote-ref-45)
46. Natalia Gulyaeva & Maria Sedykh, *Russia Enacts Data Localization Requirement; New Rules Restricting Online Content Come into Effect*, Hogan Lovells Chronicle of Data Protection (Jul. 18, 2014) *available at http://www.hldataprotection.com/2014/07/articles/international-eu-privacy/russia-enacts-new-online-data-laws/.* [↑](#footnote-ref-46)
47. Rep. and Recommendations of The President’s Review Group on Intelligence and Communications Technologies at 226-29 (Dec. 12, 2013) *available at* https://www.whitehouse.gov/sites/default/files/docs/2013-12-12\_rg\_final\_report.pdf.. [↑](#footnote-ref-47)
48. Andrew K. Woods, *Data Beyond Borders Mutual Legal Assistance Treaties in the Internet Age*, Global Network Initiative 8-12 (Jan. 2015). [↑](#footnote-ref-48)
49. *Id.* at 228. [↑](#footnote-ref-49)
50. Anonymous Interview (Apr. 7, 2015). [↑](#footnote-ref-50)
51. U.S. Department of Justice FY 2015 Budget Request. [↑](#footnote-ref-51)
52. Specifically, the DOJ requested an additional $19.6 million and 141 positions, including 77 attorneys, to staff the Criminal Division (and primarily OIA) to process MLAT requests. This would supplement previous services to support OIA functions, not specific to MLAT reform initiatives of 90 positions with 61 attorneys and $20 million. [↑](#footnote-ref-52)
53. FY 2014 had no current U.S. Attorneys services for MLAT reform initiatives. $1.3 million and 13 positions, including 8 attorneys, were requested for FY 2015 for the assignment of assistant U.S. Attorneys and support personnel in the District of Columbia and the Northern District of California to provide a dedicated team to support OIA in processing requests [↑](#footnote-ref-53)
54. FY 2014 had no current FBI services for MLAT reform initiatives. The FY 2015 request had $3.2 million and 14 positions, including 7 agents, for these FBI efforts. [↑](#footnote-ref-54)
55. Anonymous Interview (Apr. 7, 2015); [↑](#footnote-ref-55)
56. Rep. and Recommendations of The President’s Review Group on Intelligence and Communications Technologies at 228 (Dec. 12, 2013) *available at* https://www.whitehouse.gov/sites/default/files/docs/2013-12-12\_rg\_final\_report.pdf [↑](#footnote-ref-56)
57. Andrew K. Woods, *Data Beyond Borders Mutual Legal Assistance Treaties in the Internet Age*, Global Network Initiative 8 (Jan. 2015). [↑](#footnote-ref-57)
58. Rep. and Recommendations of The President’s Review Group on Intelligence and Communications Technologies at 228 (Dec. 12, 2013) *available at* https://www.whitehouse.gov/sites/default/files/docs/2013-12-12\_rg\_final\_report.pdf [↑](#footnote-ref-58)
59. *Rocket Docket*, Wikipedia (last updated Apr. 19 2015) *available at* http://en.wikipedia.org/wiki/Rocket\_docket. [↑](#footnote-ref-59)
60. *“Rocket Docket” United States District Court for the Eastern District of Virginia Frequently Asked Questions*, *available at*  http://www.leclairryan.com/files/Uploads/Documents/Rocket%20Docket%20EDVA%20FAQ.pdf [↑](#footnote-ref-60)
61. If the two steps are not formally combined, a variation would be for OIA systematically to refer MLAT requests to the same prosecutors, with the idea that the regularized nature of these referrals would operate similarly to actual combination of the two steps. [↑](#footnote-ref-61)
62. 18 U.S.C. § 2703(d). [↑](#footnote-ref-62)
63. Anonymous Interview (Apr. 7, 2015). [↑](#footnote-ref-63)
64. Rep. and Recommendations of The President’s Review Group on Intelligence and Communications Technologies at 228 (Dec. 12, 2013) *available at* https://www.whitehouse.gov/sites/default/files/docs/2013-12-12\_rg\_final\_report.pdf. [↑](#footnote-ref-64)
65. *Id.* [↑](#footnote-ref-65)
66. *Id.* [↑](#footnote-ref-66)
67. *Id*. at 228-29. [↑](#footnote-ref-67)
68. *Id*. at 229-30. [↑](#footnote-ref-68)
69. Andrew K. Woods, *Data Beyond Borders Mutual Legal Assistance Treaties in the Internet Age*, Global Network Initiative 11 (Jan. 2015). [↑](#footnote-ref-69)
70. *Id*. [↑](#footnote-ref-70)
71. http://travel.state.gov/content/visas/english/visit/visa-waiver-program.html [↑](#footnote-ref-71)
72. 8 U.S.C. § 1187(c)(2)(A). To qualify for the VWP, a country must have had a nonimmigrant visa refusal rate of less than 3% for the previous year or an average of no more than 2% over the last two fiscal years with neither year going above 2.5%. Alison Siskin, “Visa Waiver Program,” Congressional Research Service (2013). [↑](#footnote-ref-72)
73. 8 U.S.C. § 1187(c)(2). [↑](#footnote-ref-73)
74. 8 U.S.C. § 1187(c)(2)(C). [↑](#footnote-ref-74)
75. If the streamlined MLAT program appears promising to stakeholders, as we hope it will be, that could be the topic of ongoing research and discussion. [↑](#footnote-ref-75)
76. The VWP similarly requires reciprocal treatment, so that U.S. travelers receive easier entry to the other country. [↑](#footnote-ref-76)
77. http://travel.state.gov/content/visas/english/visit/visa-waiver-program.html (last visited April 17, 2015). [↑](#footnote-ref-77)
78. *Visa Waiver Program*, Wikipedia (last modified May 12, 2015), *available at* https://en.wikipedia.org/wiki/Visa\_Waiver\_Program. [↑](#footnote-ref-78)
79. We welcome ideas from readers about how effects similar to the VWP could be achieved without the need for legislation. [↑](#footnote-ref-79)
80. [cite] [↑](#footnote-ref-80)
81. The idea of an “adequate” regime in another jurisdiction, as contrasted with an identical or “equivalent” regime, has been an important issue in the ongoing discussions between the United States and the European Union about the application of the latter’s Data Protection Directive. *See* Peter P. Swire & Robert E. Litan, None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive (1998) (discussing difference between “adequate” and “equivalent” data protection regimes). [↑](#footnote-ref-81)
82. www.digitaldueprocess.org. [↑](#footnote-ref-82)
83. Smith v. Maryland, 442 U.S. 735 (1979). [↑](#footnote-ref-83)
84. United States v. Warshak, 631 F. 3d 266 (6th Cir. 2010). [↑](#footnote-ref-84)
85. United States v. Jones, 565 U.S. at \_\_ (2012) (Sotomayor, J., concurring) [↑](#footnote-ref-85)
86. [add cites] [↑](#footnote-ref-86)
87. In re: Sealed Case No. 02-001, 310 F. 3d 717 (2002). [↑](#footnote-ref-87)
88. FISA Amendments Act of 2008, Pub. L 110-261, July 10, 2008, 122 Stat. 2436. [↑](#footnote-ref-88)
89. *ICE Arrests Mafia Soldier Following Joint International Law Enforcement Operation*, (Mar. 10, 2010) (demonstrating the ability to conduct simultaneous coordinated criminal investigations in two separate countries without the use of an MLAT) *available at* https://www.ice.gov/news/releases/ice-arrests-mafia-soldier-following-joint-international-law-enforcement-operation [↑](#footnote-ref-89)
90. Anonymous Interview (Apr. 7, 2014). [↑](#footnote-ref-90)
91. *International Training*, The FBI Academy *available at* http://www.fbi.gov/about-us/training/international. [↑](#footnote-ref-91)
92. See Nairaland Forum, “Best 10 International Dating Sites of 2014”, http://www.nairaland.com/1794102/best-10-international-online-dating (discussing increasingly international nature of online dating sites). [↑](#footnote-ref-92)
93. www.airbnb.com [↑](#footnote-ref-93)
94. www.uber.com/cities (last visited April 16, 2015). [↑](#footnote-ref-94)
95. Anonymous Interview (Apr. 7, 2014). [↑](#footnote-ref-95)
96. *ECPA Reform: Why Now?*, Digital Due Process: Modernizing Surveillance Laws for the Internet Age, *available at* http://digitaldueprocess.org [↑](#footnote-ref-96)
97. [look for a better cite than Wikipedia] [↑](#footnote-ref-97)
98. [law review articles?] [↑](#footnote-ref-98)
99. [insert law review or FTC workshop reports on identity theft in the US, where the same complaint that the city where the fraudster lives doesn’t care about the citizen from a distant city or state] [↑](#footnote-ref-99)
100. [cite US wiretap law for payments; law review cite if possible to the practice generally; research question how cross-border wiretaps have been funded] [↑](#footnote-ref-100)
101. Dave Lavinsky, *Pareto Principle: How to Use it to Dramatically Grow Your Business*, Forbes (Jan. 20, 2014, 9:39AM) *available at* http://www.forbes.com/sites/davelavinsky/2014/01/20/pareto-principle-how-to-use-it-to-dramatically-grow-your-business/ [↑](#footnote-ref-101)
102. Mancur Olson, The Logic of Collective Action: Public Goods and the Theory of Groups (1965). [↑](#footnote-ref-102)
103. A fifth funding proposal would need further thought to turn into a concrete proposal. For enforcement against certain kinds of trademark violations, owners of the mark can fund special magistrates who can conduct the investigation. [cite] There may be ways that requesting countries can send details to receiving countries or otherwise fund or support investigative activities in the receiving countries in ways that would correct for the lack of incentive to investigate for the receiving country. [↑](#footnote-ref-103)