Problematic Alternatives: MLAT Reform for the Digital Age

By branden / January 28, 2015

Jonah Force Hill

I. Introduction

As criminals (and their victims) increasingly communicate and store data online, law enforcement officials correspondingly seek greater access to digital information for criminal investigations and prosecutions. But this information is often stored on servers around the world and moves without consideration of national boundaries. Retrieving critical information has become vastly more challenging for law enforcement because data globalization has blurred jurisdictional lines and rendered prior evidence-gathering methods and procedures largely ineffective.

This difficulty causes international conflicts: governments, tech firms, and the legal community all seek to reconcile data globalization with competing demands for national sovereignty, citizen privacy, corporate responsibility, and a robust criminal justice system – and all under the watchful eyes of an international public still profoundly wary of government overreach in a post-Snowden world.

Ameliorating this tension requires reforming the Mutual Legal Assistance Treaty (MLAT) process, the system of bilateral and multilateral agreements by which nation states commit to assist one another in criminal investigations and prosecutions. The MLAT system today is deeply dysfunctional. Responses to MLAT requests for information are often abysmally slow; many of the requests are denied or only partially satisfied due to confusion over the rules governing data. Consequently, governments cannot rely on MLATs to acquire digital information for their criminal cases, and they are beginning to consider alternatives. These alternatives, however, run the risk of damaging international cooperation on criminal justice issues and of fragmenting the global Internet ecosystem. Governments must urgently—yet thoughtfully—reform the MLAT system before alternatives to MLATs become the norm.

Using *Microsoft v. United* States as a case study, this article highlights some problems with the current MLAT system, explains the risks of inaction and the benefits of MLAT reform, and recommends policy solutions.

II. Background: MLATs

MLATs are a cornerstone of global cooperation on law enforcement and one of the most widely used **mechanisms** for requesting foreign assistance in domestic criminal investigations and prosecutions. MLATs are broadly worded to allow for **cooperation** on a wide range of law enforcement issues, like locating and extraditing individuals, freezing assets, requesting searches and seizures, and taking testimony. They are an **effective** tool in combatting transnational crime like money laundering and human trafficking, and prosecuting criminals who attempt to evade domestic law enforcement by operating abroad.

But the MLAT system has struggled to keep pace with globalized data. The number of MLAT requests has skyrocketed and the matters they concern have grown vastly more complex. The United States Department of Justice (DOJ) **estimates** that over the past decade the "number of MLAT requests for assistance from foreign authorities has increased by nearly 60 percent, and the number of requests for computer records has increased ten-fold." Many of today's MLATs were drafted before globalized data and therefore do not address core questions of data jurisdiction, like how to treat data held overseas by a subsidiary of a domestic parent company. Perhaps most significantly, many **MLATs** do not effectively address fundamental issues like notions of privacy versus law enforcement's need for evidence. For example, MLATs frequently do not specify what constitutes "protected data" or under what conditions "content" differs from "metadata" for the purposes of information sharing. This hinders cooperation between states with differing domestic understanding of these terms.

The increase in MLAT requests and legal uncertainty surrounding privacy and data protection regulations have significantly delayed the MLAT process. The President's Review Group on Intelligence and Communication Technologies (the independent review board tasked with assessing U.S. intelligence collection practices following Snowden) **estimates** that it takes an average of ten months for DOJ to process MLAT requests, and can take years. Foreign countries' MLAT requests are similarly drawn out, and can take far longer. Such delays are unacceptable to law enforcement officials who urgently need information. Unsurprisingly, impatient prosecutors are looking for MLAT alternatives. However, those prosecutors and their governments must be mindful of the potential long-term consequences of those alternatives, particularly adverse consequences to the functioning of the Internet itself.

III. *Microsoft vs. United States*: Circumventing MLATs Through Expanded Jurisdiction

The ongoing *Microsoft v. United States* case demonstrates this frustration. The Justice Department is seeking information from a Microsoft Outlook account based in Ireland for a criminal investigation in the Southern District of New York. Instead of pursuing that account through an MLAT request to Irish authorities, like prior practice, prosecutors sought a **warrant** instructing Microsoft to produce information from the account directly. Microsoft challenged the warrant, but the District Court (after substantial briefing, including amicus briefs submitted by other large Internet and telecom companies) sustained the issuance. Microsoft is **appealing** that ruling before the Second Circuit Court of Appeals.

DOJ made a policy choice to seek a warrant rather than using the MLAT process, based in large part on concerns about the efficacy of the MLAT system and the potential for a drawn-out waiting period. In its brief to the District Court supporting the warrant, the government **argued**, "[i]n contrast to an SCA warrant [the statutory form of warrant issued], which can be served upon a provider immediately upon issuance by a judge, an MLAT request typically takes months to process, with the turnaround time varying widely based on the foreign country's willingness to cooperate, the law enforcement resources it has to spare for outside requests for assistance, and the procedural idiosyncrasies of the country's legal system." The Federal Magistrate ruling in support of the government's issuance of the warrant likewise **noted** that the "slow and laborious" MLAT procedures placed such a "substantial" burden on the government as to necessitate other means of retrieval. In other words, the government, the Federal Magistrate, and the District Court all rejected Microsoft's contentions and accepted the view that MLAT did not offer a satisfactory means of obtaining evidence and a warrant was a necessary alternative, notwithstanding extraterritoriality concerns.

Microsoft's challenge is premised on the legal assertion that the government warrant does not permit extraterritorial searches, but two policy considerations are also central to its position. First, like many other major American technology companies, Microsoft faces the perception, post-Snowden, that U.S. tech firms have been complicit in—or at least overly submissive to—NSA intelligence collection programs and therefore cannot be trusted to protect foreign customers from American government overreach. Microsoft **protested** the warrant in part because of its desire to be seen to maintain a degree of independence from the U.S. government as well as protect the rights and privacy of its non-American customers.

Secondly, and perhaps more importantly, Microsoft recognized circumvention of the MLAT process sets a troubling precedent for future extraterritorial data requests (a view **shared** by the Irish government). By attempting to treat data stored abroad like domestic data, Microsoft contends, DOJ is dramatically expanding its reach into foreign states—states with sovereign laws governing digital information stored within their borders. It is also subjecting American firms with data stored abroad to multiple and potentially contradictory data protection rules. Given the push by nations around the world, most critically within Europe, to update domestic data protection laws in ways that diverge significantly from American rules, Microsoft **argued** that forced compliance with multiple and inconsistent discovery and disclosure requirements could result in endless stream of legal battles for tech firms operating abroad and perhaps force American companies to entirely pull out of certain markets.

The government has a legitimate interest in obtaining this information for its criminal investigations, and Microsoft has equally compelling reasons to resist providing information to the United States in potential violation of privacy or data protection laws of foreign countries where it operates. These possible international investigatory conflicts spawned the MLAT system in the first place. Yet this case arose precisely because the government concluded —probably rightly—that MLAT would not meet its needs. *Microsoft* shows in the starkest light that MLATs are inadequate to law enforcement in the digital era.

IV. Foreign States: Reforming Domestic Law to Increase Data Access

Foreign states have also encountered MLAT problems. The Brazilian government has been **frustrated** by extended delays in the MLAT system, especially pertaining to its request for information from Google's American servers for several cases pending before the Brazilian Supreme Court. India similarly **has found** the MLAT process with the United States to be ineffective. It has often invoked the U.S.-India MLAT to request that America serve summonses on Google, Facebook, Twitter, and others for failing to prevent the dissemination of online speech prohibited under Indian Law, but these requests have been repeatedly **rejected** due to U.S. civil liberties sensibilities.

However, there are asymmetries between the U.S. government frustration with the MLAT process and non-American frustration. American tech firms maintain the lion's share of the global data storage marketplace. When Brazilians, Indians, or others find that they cannot get timely access to the data they want, in theory they can issue a direct subpoena or warrant under domestic law. But unlike the Americans, they generally have to issue those direct requests to a subsidiary that may not "possess" the desired information. Even if the parent/subsidiary problem does not arise, those governments have less influence over the American parent company than the U.S. government, because the presence of the headquarters, boards of directors, and principal officers of these companies in the United States makes them particularly susceptible to discovery efforts of American prosecutors.

Foreign governments are understandably frustrated by this asymmetry. Legislatures and regulators are consequently considering new legal **regimes** that would either keep data local or establish local jurisdiction over all citizen data no matter where it sits. Germany, for example, is considering server and data localization as part of a new **Internet security law**. In Brazil, the Internal Revenue Service announced its Declaratory Act #7 in October 2014 that would

impose a 50% tax on all tech companies holding data overseas. These laws would partly mitigate the asymmetry by allowing for discovery of information directly from the subsidiary in the same manner as DOJ demanded in the Microsoft case.

Both alternatives to MLATs—localization and jurisdictional expansion—are deeply problematic. First, forcing companies to hold data domestically (or to insist that only domestic firms operate domestically) will likely raise Internet user and small business costs and reduce the ability of firms to aggregate services and data analytics through cloud services. Equally important, localization policies will probably degrade data security by making censorship and surveillance easier for domestic governments (and perhaps even foreign governments).[1] Jurisdictional expansion will subject companies to multiple and often competing jurisdictions, and may force firms to leave certain markets. Under either of these scenarios, Internet companies suffer, Internet users suffer, and privacy and Internet freedom may suffer as well.

V. Policy Recommendations

These MLAT alternatives are potentially harmful to a robust and free Internet, and could be rendered unnecessary by appropriate MLAT reforms like the following.

A. Increase MLAT funding

Insufficient resources are a primary cause of MLAT backlogs. The United States must spend more money to make MLATs work for foreign law enforcement. America's recent $24 million in new funding was necessary but insufficient. More MLAT requests will come in as criminal prosecutions increasingly focus on digital evidence. The United States is also entitled to expect other countries to spend more to expedite responses to American requests. Realistically, other nations must recognize that American prosecutors will turn to warrants like in *Microsoft* if their MLAT requests gather dust in foreign justice ministries.

B. Issue unilateral guidelines for direct data requests

Governments should issue unilateral, self-binding guidelines to limit prosecutors' authority to bypass an applicable MLAT and compel production of electronic records stored outside their own jurisdiction. For instance, when the information sought is particularly sensitive (perhaps political or financial information) governments should unilaterally require that prosecutors use MLAT procedures. Further, once increased resources (recommendation #1) speed up the MLAT process, governments ought to consider instituting a "first use" constraint, requiring that law enforcement agencies try in good faith to use to the MLAT process prior to pursuing direct access. A "first use" constraint, of course, is likely to be politically palatable only among nations that adopt parallel reciprocal procedures.

C. Streamline the MLAT process

The MLAT review process should be reformed and streamlined. There are no online submission forms for MLAT requests today. MLATs must either be submitted by paper or by email to relevant authorities in a slow and cumbersome process. All nations with MLATs should create an online submission form and guide. As the President's Review Group has noted, the current MLAT process also contains multiple, often redundant, request reviews. For instance, the U.S. DOJ's Office of International Affairs and the U.S. Attorney's Office must conduct separate, independent reviews. Such redundancies should be reevaluated for efficacy and necessity.

D. Adopt industry-wide legal interpretations for data requests

Major technology and Internet firms should seek industry-wide consensus on how to interpret national and international law on data collection from law enforcement authorities. This industry-wide statement will not necessarily alter the way in which governments seek to access data, but it will give law enforcement a sense of the types of requests that will be challenged versus the types of requests that are broadly seen as appropriate. This could help avoid unnecessary legal and political confrontations.[2]

E. Renegotiate existing MLATs

Tech sector innovation and data globalization has complicated former notions of jurisdiction. Nevertheless, agreement can be reached on key terms and principles in a sufficiently broad way as to avoid bottlenecks in the MLAT process. These key terms and principles must be incorporated into updated MLAT agreements. To ensure that MLATs keep pace with changing technologies, provisions dealing with data issues should be revisited frequently within multi-national working groups.[3]

V. Conclusion

Reforming the MLAT system is tremendously important to inter-state law enforcement cooperation and the future of the global Internet more generally. If left unreformed, or reformed poorly, law enforcement and jurisdictional battles among and between governments and technology firms could place yet

another strain on the already stressed global Internet system. By contrast, developing updated and efficient MLATs could pay enormous dividends, not only for law enforcement as it faces enormous international challenges, but also by serving as confidence-building measures as sovereign nations take on the task of resolution of other, even more difficult, global Internet policy challenges. The question is whether or not governments will take the steps necessary to expedite and modernize the MLAT system before alternatives do irreversible damage to the international system.

Jonah Force Hill writes on Internet policy and cybersecurity issues, and formerly served in the White House Office of the Cybersecurity Coordinator and as a Cybersecurity Teaching Fellow at Harvard. The views expressed are entirely his own.

[1] Data stored abroad may be more vulnerable to access by foreign intelligence agencies because those agencies often have fewer restrictions on their activities abroad than in their home nations. For example, the NSA has a substantially broader remit to conduct surveillance outside of the United States than within.

[2] The technology policy advocacy group, *Access*, has suggested that the tech industry should publically explain their "interpretation of the law and the way in which they exercise their discretion as to when, how, and under what conditions user information is provided." "Discussion paper – What are the solutions to the 'MLAT problem'?" *Access*. Available at https://mlat.info/policy-analysis-docs/discussion-paper-what-are-the-solutions-to-the-mlat-problem

[3] For example, as "data sharding" architectures becomes increasingly prevalent (data sharding is the process of partitioning data into pieces and dispersing them across multiple databases — oftentimes situated on servers located around the globe) or database caching (storing databases as temporary cache files), states may need to revisit notions of data "location," data "type," "personally identifiable information," etc., within their respective treaties.

← PREVIOUS
Restricted Reporting on California Military Installations: The …

NEXT →
Volume 6, Issue 1

The Harvard National Security Journal

The Harvard National Security Journal (NSJ) is the nation's leading journal in the field of national security and law. The main edition publishes scholarly, practical articles by professors, legal practitioners, and national security professionals twice a year. The online edition publishes scholarly essays throughout the academic year.

The Harvard National Security Journal is an officially recognized student-run journal of Harvard Law School. Membership in this journal is open to all HLS students.