MLAT REFORM: A STRAW MAN PROPOSAL

Greg Nojeim, Director of the Freedom, Security and Technology Project at the Center for Democracy & Technology.

As more and more data flows across state borders, the ability of law enforcement agencies to access information stored outside their jurisdiction or managed by a foreign company becomes increasingly complex. What country's laws should apply to data requests? How quickly should access be granted and to whom? Should there be different standards for different countries? Mutual Legal Assistance (MLA) processes have been one way to address these questions.

MLA processes are those that law enforcement officials in one country trigger in another country to gain access to information over which the 2nd country has jurisdiction. The information sought may range from witness testimony to communications content and metadata. For example, if an investigating official in France needs communications content of a Gmail user in France to investigate a crime, she does not make the request directly to Google, but rather approaches a central authority in France which makes a request for mutual legal assistance of the US Department of Justice (DOJ), which can provide that assistance by applying for a warrant to serve on Google to compel disclosure of this information.

It is widely perceived that MLA processes are too slow for law enforcement investigations in the digital era and that they are not up to the task of dealing with the volume of cross-border demands for data that law enforcement agencies need to make. A number of ideas are being put forth to address this problem and its many complexities. This post is an attempt by the Center for Democracy & Technology (CDT) to spur public debate on one such idea and to solicit input that would inform a solid MLAT reform proposal.

Background

Many MLA processes are captured in treaties called MLATs. MLATs are used only for criminal investigations, not for intelligence surveillance. Foreign governments often complain that US MLAT processes work too slowly and inefficiently. The average turn around time for an MLAT request filed by a foreign country with the US is approximately 10 months, according to the President's Review Group on Intelligence and Communications Technologies (p. 227). Foreign governments file approximately 3,000 MLAT requests each year with the US and a significant portion of those requests are for data held by US providers. The US files approximately 1,000 MLAT requests/year with foreign governments.

The DOJ Office of International Affairs receives and makes MLAT requests for the US. It receives foreign requests, seeks a judicial order (such as a warrant) when necessary, gathers the information from a company, and then furnishes it to the foreign

government. The DOJ plays an important role in ensuring that an MLAT request from a foreign government is proper and that fulfilling the request would not violate free speech rights. The DOJ also works with a US Attorney to file any necessary warrant application and in works with the FBI to remove irrelevant communications from any response to the foreign government before it is provided. Read more about MLATs and Mutual Legal Assistance here and here.

Interplay of MLATs and US surveillance law

The Electronic Communications Privacy Act (ECPA), as interpreted by both the DOJ and major US providers, prohibits companies from disclosing communications content to foreign governments absent a warrant issued by a US judge based on a finding of probable cause. A huge proportion of the requests for assistance that DOJ receives from foreign governments for content are turned back because the requesting entity has not provided enough facts to reach the probable cause threshold. This causes delay.

Under 18 USC 2702(c)(6) and 2711(4), ECPA does not prohibit US communications service providers from disclosing non-content to foreign governments at will. Different companies employ different rules when considering whether to make a voluntary disclosure of non-content to a foreign government. Company transparency reports often reveal the extent of these disclosures. When a provider exercises its discretion to turn down a non-content request from a foreign government, the foreign government may seek the data through an MLAT or other MLA process.

While MLAT agreements do not themselves typically impose dual criminality requirements, 18 USC 3512(e) indicates that ECPA warrants will be sought in connection with foreign government requests only when the conduct being investigated by the foreign government would be a felony in the US.

Disagreement about jurisdiction over data

There is disagreement about what is the best test for determining which country has jurisdiction over data. This makes it difficult to decide as a threshold matter which country's law governs access to the information in question, thus complicating the MLAT reform debate. Options for a jurisdiction test include: location of the data, citizenship of the data subject, location of the data subject, place the crime occurred, and place of incorporation (or major operations) of the company holding the data. All these options have problems. See, for example, Professor Orin Kerr's discussion on pp. 416-418 in this article. Location of data, for example, may not be a good test because data are so mobile. Citizenship of the user may not be a good test when the user is a citizen of a repressive country, and because citizenship will not be known by a provider and may not be known by the requesting government. Rather than try to resolve this complex issue, the approach taken here assumes that a country that has jurisdiction over data held by a communications service provider headquartered in that country.

One Possible Approach To Reform: *Subjecting "wholly domestic" MLA requests from certain countries primarily to the requesting country's domestic law could serve as a partial solution.*

One approach that would reform MLA processes for some requests would be to amend ECPA to permit certain requests for communications content and transactional records from foreign governments to be made *primarily* under the foreign government's surveillance laws, if those laws meet baseline human rights standards and provide reciprocal treatment of corresponding US MLA requests. Because of the circuit breaker role DOJ would continue to play, and because providers would be permitted – not required – to make disclosures to foreign governments, the requests would not be made solely under the requesting country's laws.

Primarily domestic law treatment would apply only to "wholly domestic" MLA requests: those in which the citizenship and location of the alleged victim, perpetrator and data subject are all the same country, and the crime occurred in that country. The only nexus to the US would be corporate headquarters of the company holding the data, no matter where the data are stored. Presumed location of the data subject would be determined by IP address, though it is imperfect for this purpose.

This is a limited class of cases and it is unclear what proportion of the US MLAT backlog it would address. However, it would deal with the cases where application of current US standards and US procedures are most objectionable to foreign governments.

Treatment of non-content: This proposal would smooth and speed access to communications content by making it available – with some exceptions – under the requesting company's laws. For certain non-content requests, it would impose a standard where there is none now. The more sensitive non-content – transactional records such as email logs – which providers can now disclose voluntarily to foreign governments regardless of whether the request meets the requirements of the requesting country's domestic law, would be treated like content: no voluntary disclosure would be permitted to countries that qualify for primarily domestic treatment of content requests. Instead, such disclosures, like content, would be made primarily under domestic law. Special allowance would be made for emergency requests. Subscriber information such as temporarily assigned IP address, which may now be disclosed by providers to foreign governments voluntarily, would be treated no differently under this proposal than it is today. Providers could agree to industry standards for disclosure of this information.

Role of the DOJ and of Courts. Wholly domestic requests by governments whose surveillance laws meet baseline human rights standards would not be subject to US judicial review. To the extent there is judicial authorization, it would be that required by the law of the requesting country. The DOJ would act as the circuit breaker at the back end for inappropriate requests for content and transactional records. While the initial

request would go directly to the provider with notice to DOJ, the provider would make its disclosure to DOJ, which would continue to play the role it now plays in enforcing dual criminality requirements (including filtering out requests related to "speech crimes"), ensuring that information is not sought in connection with a human rights violation, blocking requests that do not comply with the requesting country's laws, and working with the FBI to remove non-responsive information before a request is fulfilled.

Content of baseline human rights standards: What the baseline human rights standards would be would need to be established, as would a mechanism for determining whether the standard has been met. The *Necessary and Proportionate Principles*, which CDT has endorsed, would guide these standards, but as no country's surveillance laws fully conform with these principles, there will have to be some flexibility. The mechanism for determining whether the standard has been met would involve the DOJ, but would likely also have to involve an entity respected internationally for upholding human rights values in an objective way and without favoring one country over another.

Reciprocity. To gain the benefits of this proposal, a country would have to offer reciprocal treatment to the US government. The US government's "wholly domestic" requests for content and transactional records held by providers headquartered abroad would have to meet primarily the requirements of US law, not those of the country in which the provider has its headquarters.

Benefits of this partial solution:

- It creates an incentive for countries to increase surveillance standards to meet the human rights requirements that would have to be met in order to gain access to communications content in the cases covered.
- It facilitates investigation of wholly domestic crimes by permitting requesting countries with laws that meet human rights standards to seek information pertaining to those crimes primarily under their own laws.
- It lessens pressure for data localization mandates. To the extent it addresses concerns of foreign governments that they are unable to investigate wholly domestic crimes because they cannot gain access under their own laws to information held by US providers, it diminishes the pressure to address such concerns by requiring providers to locate data domestically.
- It ends the "Wild West" for requests for transactional records from foreign governments. It gives solid guidance to companies that receive such requests. Their disclosure of such information would still ultimately be voluntary: ECPA would be amended to permit the disclosure to foreign governments of transactional records and content, not to mandate it.
- The proposal deals with the class of investigations in which the US has the least interest in imposing its own standards. Neither the crime perpetrator, crime victim or crime locus is in the US, or, in the case of perpetrators and victims, is a US entity. More difficult cases would be addressed in other solutions.

- DOJ would retain its authority as a circuit breaker for inappropriate requests.
- US demands for content and transactional records held by a company headquartered in a consenting country, in wholly domestic cases, would be governed primarily by ECPA, thus facilitating such investigations.
- The proposal does not require a new treaty or a series of new bi-lateral treaties. An amendment to US law would be all that is required.

Possible Drawbacks:

- The standards the US imposes for content requests are generally higher than (or at least are different from) those in the rest of the world. Requiring independent judicial authorization for law enforcement access to communications content may be rare, and "probable cause" is a higher level of proof than most countries require. See this report and chart. For requests from these countries for these crimes, the standard that would have to be met would be reduced.
- Countries that do not meet the baseline human rights standard would not benefit from the partial solution, which could feed the perception that the US and countries that meet the standard have outsized control over the Internet and impact other issues, including governance and data localization mandates.
- Countries with which the US has friendly relations may have surveillance laws that do not meet baseline human rights standards. They may be reluctant to change their laws to meet such standards, thus putting downward pressure on the standards themselves.
- It may be difficult to establish baseline human rights standards that are widely agreed to, and even more difficult to select or create the entity or entities that would decide whether the standards have been met.
- Removing DOJ's obligation to file warrant applications for some content will reduce its burdens, but giving DOJ circuit breaker responsibility for requests for transactional records that providers now disclose voluntarily will increase its burdens, and, depending on the volume of those demands, could slow rather than speed up MLA responses.
- The proposal does not address crimes other than the wholly domestic crimes, and more and more criminal activity has cross-border elements. As such, it is a partial solution, and perhaps an interim solution, while a more comprehensive approach that involves a new treaty (or treaties) is negotiated.

Conclusion

CDT neither supports nor opposes this proposal and it should not be characterized as a CDT proposal. We see some plusses and minuses. Instead, we put it forth in order to solicit commentary that would inform any actual proposal that CDT and others might make. We also put it forward to inform the debate about MLAT reform in a larger sense because variations of the ideas discussed here are being considered by others. We are hopeful that the response to this proposal will inform those reform efforts as well. *[For further information, contact Greg Nojeim at gnojeim@cdt.org; 202/637-9800.]*