EVALUATING MLATS IN THE ERA OF ONLINE CRIMINAL CONDUCT

Shalini S

Research Fellow

CCG Working Paper Series (2015-16)

Number 2

A Mutual Legal Assistance Treaty (MLAT) is often the first instrument to be invoked by law enforcement officers in cases of transnational crime. As crime is becoming progressively globalized, domestic law is insufficient to undertake satisfactory investigation and prosecution. International assistance measures, like MLATs, have become necessary for effective law enforcement. But, are MLATs effective in securing investigative cooperation and evidentiary data for new-age criminal activity such as computer crime? Is there scope for effective MLAT reform or is it time to imagine newer means of extending and receiving international assistance in such criminal investigation?

Transnational Nature of Cybercrime and its Implication for Investigative Agencies

India is facing a large number of cyber-attacks, launched from within and outside its borders. In pursuing investigations in these cases, India routinely faces difficulties in gaining access to cross-border data held by US and UK agencies and internet service providers (Joshi 2013). Generally, investigation of any cross-border criminal conduct often necessitates the gathering of evidence located in foreign jurisdictions. However, jurisdictional limitations preclude domestic law enforcement agencies from locating and retrieving evidence based in other countries. The right of each sovereign to enforce the rule of law, to proscribe conduct and award sanctions in case of violation, cannot be infringed.

Legal sovereignty of states extends to cyberspace (Betz and Stevens 2011:58) and states do exercise jurisdiction over conduct in cyberspace (Trachtman, 1998:568-569). States even exercise exclusive territorial jurisdiction over cyber infrastructure located within their borders (Heinegg, 2013:134). However, criminal conduct in cyberspace does not necessarily occur in the territory of a single sovereign (Brenner, 2006:190). This means the operation of jurisdiction of several states can simultaneously be attracted. Jurisdictional determination is challenging in cases of cybercrime as the criminal, the victim, means and the effect of the crime are all capable of existing in different countries (Brenner and Koops 2004:44). Due to this, cross-border cooperative measures become necessary in conducting criminal investigation in cybercrime cases.

Therefore, lawful access to data located in another state's jurisdiction can only be gained by requesting assistance of the country exercising jurisdiction over this data. International cooperation from the country that can legally compel disclosure of the data is critical in conducting effective cybercrime investigation. This is also demonstrated by the fact that mutual legal assistance is enshrined in and facilitated by provisions of Budapest Convention on Cybercrime. While states are unwilling to yield territoriality in cyberspace, they seek to be mutually cooperative in combatting transnational cybercrime to ensure a safe cyberspace.

What are MLATs?

MLATs are bilateral or multilateral treaties that can be negotiated to allow for an array of formalized legal assistance measures between countries. These include search and seizure, witness statements, facilitation and confiscation of evidence, and service of documents of extraterritorially located information. MLATs are often "negotiated on a country-to country basis" (Ghosh and Turrini 2010:321) and generally aid ongoing criminal investigations and proceedings. They are a primary form of seeking international legal assistance and have been used multiple times to extend and receive digital evidence in cybercrime investigations (Westby 2003:100). MLATs can potentially allow access to data that may not be accessible in a domestic investigation, as they can bypass domestic protections like the judiciary and safeguards to access. However, MLATs are not the only means of seeking assistance to gain transborder data access.

Distinguishing MLATs from other international legal assistance measures

To effectively police cybercriminal conduct, countries are often forced to request some form of international law enforcement cooperation and assistance. If voluntary and informal assistance is denied, countries can resort to MLATs, letters rogatory or extradition agreements.

Letters rogatory or letters of request are customary methods of international cooperation. They are exchanged between judicial agencies to seek cross-border investigation assistance

in ongoing proceedings. It seeks the performance of an act which needs the sanction of a foreign court (Brenner and Schwerha 2004:112). These can be employed even when no MLAT has been effectuated between countries. In Indian law, Sec. 166A and Sec 166B of the Code of Criminal Procedure outlines the power of Indian courts to advance and receive letters of request.

MLATs and letters rogatory processes rely on countries mutually assisting each other through national investigation and exchange of information and evidence. However, requests under the letters rogatory process are more time-consuming and less reliable than requests advanced through the MLAT process (Brenner 2012:180). This is because MLATs impose international legal obligations on the state receiving the request for assistance whereas letters rogatory only serve as a request for assistance that states need to respond to. (Watson 1992:75). In addition to these measures, extradition treaties may help in securing identified cybercriminals and subjecting them to trial.

While the letters rogatory process is often criticized for being unable and unwilling to provide accurate digital evidence in a timely manner, MLATs are only marginally better. As online crime and digital evidence bear features distinct from physical crime and evidence, the MLAT process also face difficulties in facilitating notable international law enforcement cooperation.

Unique Challenges of using MLATs in Cybercrime Investigations

1. MLATs premised on the principle of dual criminality

Some MLATs may impose a general dual criminality requirement (conduct criminalized in both countries) or require the dual criminality standard to be met for certain kinds of assistance (Bassiouni 2008:389). Cybercrime can broadly be understood to refer to any45Zcriminal activity facilitated or committed through a computer, network or hardware device (Gordon and Ford 2006:14). However, as the exact definition and classification of different cybercrimes vary across countries, some online conduct may only be criminalized by one of the parties to the MLAT. In such cases, MLATs cannot be used by requesting states to gain assistance, as the dual criminality standard is not met. Further, even in cases where there is no dual criminality provision governing mutual assistance, criminal

investigation and prosecution may not be possible. This is because an assisting state may not be able to investigate or prosecute an act which is not deemed criminal in its jurisdiction (Bassiouni 2008:389), a possibility in the absence of a dual criminality obligation.

2. Complexity of managing electronic evidence requests

Electronic data is capable of being forged, altered, deleted or destroyed and must be retrieved at the earliest. However, the MLAT process is too time-consuming to be able to capture electronic data effectively. It has many levels of bureaucratic approval requirements before the requested evidence is collected and transmitted to the requesting authority. The paperwork of an MLAT request is checked for compliance in both, the requesting country and receiving country, further increasing the time required in processing these requests. This is problematic as electronic evidence can be lost or altered in the time between advancing the request and receiving approval for the capture of data.

Additionally, the fact that the requesting attorney has little oversight and must rely entirely on foreign investigation is a key drawback of the MLAT process. The manner in which electronic evidence is handled by foreign countries cannot be challenged (Kent 2015).

MLAT Reform for Electronic Age

The time delay in processing requests and the inefficiency with which digital data is retrieved in the current MLAT process renders it an ineffective law enforcement cooperation tool. There is a need to reform the MLAT process, to make it an effective instrument in transnational cybercrime investigation. MLAT procedures must be simplified and streamlined to ensure speedy compliance checking and processing. A time limit must be stipulated, within which governments must be required to capture and provide online data to the requesting state. Law enforcement officers and attorneys must be sensitized to the nature of data that can be accessed through MLAT and the correct manner of advancing these requests. There must be increased transparency in the entire MLAT process that allows the requester to track the status of a transborder data access request. Few countries have also demonstrated a lack of political will in sharing data that is critical to a criminal investigation in a foreign country. This should not impede international law enforcement cooperation and the MLAT process must be made more equitable. MLAT agreements must be reviewed at

regular intervals to adapt it to any relevant technological advances. India must renegotiate its MLATs with countries like US and UK to ensure that a majority of India's requests for cross-border data access are honoured.

Bibliography

1. Sandeep Joshi, NSA scoffs at Indian Prism, favours cooperation on cyber security, July 22, 2013, The Hindu, http://www.thehindu.com/news/national/nsa-scoffs-at-indian-prism-favours-cooperation-on-cyber-security/article4938279.ece
2. Betz, David. J and Tim Stevens (2011): *Cyberspace and the State: Toward a Strategy for Cyber-Power,* London : Routledge.
3. Trachtman, Joel (1998): "Cyberspace, Sovereignty, Jurisdiction, and Modernism," *Indiana Journal of Global Legal Studies,* Vol 5, No. 2, pp 561- 581.
4. Heinegg, Wolff (2013): "Territorial Sovereignty and Neutrality in Cyberspace," *International Law Studies,* Vol 89, pp 123- 156.
5. Brenner, Susan (2006): "Cybercrime Jurisdiction," *Crime, Law and Social Change,* Vol 46, No. 4, pp 189-206.
6. Brenner, Susan and Bert-Jaap Koops (2004): "Approaches to Cybercrime Jurisdiction," *Journal of High Technology Law,* Vol 4, No.1, pp 1-46.
7. Westby, Jody (2003): *International Guide to Combating Cybercrime,* American Bar Association.
8. Ghosh, Sumit and Elliot Turrini (2010): *Cybercrimes: A Multidisciplinary Analysis,* Springer.
9. Brenner, Susan and Joseph Schwerha (2004): "Introduction—Cybercrime: A Note on International Issues," *Information Systems Frontiers,* Vol. 6, No.2, pp 111-114.
10. Brenner, Susan (2012): *Cybercrime and the Law: Challenges, Issues, and Outcomes,* Boston: UNEP.
11. Watson, Geoffrey (1992): "Offenders Abroad: The Case for Nationality-Based Criminal Jurisdiction," *Yale Journal of International Law,* Vol 14, No. 71, pp 41-84.
12. Bassiouni, Cherif (2008): International Criminal Law, Volume 2 Multilateral and Bilateral Enforcement Mechanisms, Leiden: Brill.
13. Gordon, Sarah and Richard Ford (2006): "On the definition and classification of cybercrime," *Journal in Computer Virology,* Vol 2, No. 1, pp 13-20.

14. Gail Kent, The Mutual Legal Assistance Problem Explained, Feb 23, The Center for Internet and Society at Stanford Law School Blog, http://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained