International Chamber of Commerce
The world business organization

Policy statement

Prepared by the ICC Commission on
the Digital Economy, Task Force on Internet and Telecommunications

Using Mutual Legal Assistance Treaties (MLATs) To Improve Cross-Border Lawful Intercept Procedures

Highlights

- Communications trends like mobility and cloud computing present increasing challenges for cross-border lawful intercept
- MLATs are a key tool for addressing these challenges
- ICC offers ten recommendations for MLAT improvement, covering (1) geographic and substantive scope of MLATs, (2) efficient MLAT processes, and (3) education and transparency

Document No. 373/512 – (12 September 2012)

I. Background – Challenges of Cross-Border Lawful Intercept

The ICC Commission on the Digital Economy has recognized as a top priority the need for governments and the private sector to establish a responsible balance of interests for lawful intercept (LI) on both national and cross-border bases. ICC has also emphasized that, in addition to providing for LI with appropriate authorization to enforce national laws, governments must ensure that the use of LI is consistent with other important legal obligations and goals of consumers and businesses, such as information security, human rights, and privacy, transparency and proportionality.

This policy statement continues the Commission's work on LI, offering recommendations for improvements to mutual legal assistance treaty (MLAT) processes, in order to improve the effectiveness of cross-border LI procedures and reduce unnecessary and disproportionate burdens. The Commission on the Digital Economy acknowledges the significant past efforts of governments and law enforcement agencies (LEAs) to negotiate and use MLATs, and believes that substantial further opportunities remain for expanding and improving MLATs, as well as cross-border law enforcement cooperation more generally. This policy statement provides recommendations and a proposed model approach for doing so.

ICC has produced two recent policy statements on LI and related topics:

- *ICC policy statement on global business recommendations and best practices for lawful intercept requirements* (June 2010); http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2010/ICC-policy-statement-on-Global-business-recommendations-and-best-practices-for-lawful-intercept-requirements/**;** and
- *ICC policy statement on cross-border law-enforcement access to company data – current issues under data protection and privacy law* (February 2012), http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2012/ICC-policy-statement-on-cross-border-law-enforcement-access-to-company-data-%e2%80%93-current-issues-under-data-protection-and-privacy-law/

A central focus of these policy statements is on cross-border LI, which is rapidly increasing in importance and frequency due to the on-going evolution of electronic communications infrastructure and services (including mobile services, cloud computing, machine-to-machine communications, and social media) coupled with a material increase in cross-border criminal activity (including both cybercrime and terrorism). As a result of these global trends, it has become very common for LEAs to have genuine and urgent needs for access to communications content and data located outside of their jurisdictions, leading to a substantial increase in cross-border LI requests.

Cross border LI presents two main challenges for communications service providers (CSPs), especially those that operate in multiple countries:

- **differences in legal and technical LI requirements** among countries, which present significant compliance issues and costs, including because of the need to implement different LI technical solutions in different places and because the requirements themselves are often not particularly transparent; and
- **inconsistent legal requirements** that can arise where cross-border communications are subject to the jurisdiction of LEAs in multiple countries, particularly where LEAs make extra-territorial requests to CSPs (e.g. where data regarding a communication sought by an LEA in Country A are stored in Country B).

ICC's June 2010 LI policy statement began to consider these issues, making two recommendations focusing on the first challenge of differing legal requirements:

- **Recommendation 4** – "LI laws, regulations and standards should be consistent across borders, and utilize international technical standards"; and
- **Recommendation 5** – "Centralized, multi-country LI solutions should be permitted".

MLAT improvement, the focus of the present statement, can help address these recommendations by increasing the interoperability of international LI requirements. Moreover, MLATs can even better address the second challenge of inconsistent legal requirements, by substituting cooperation between LEAs in different countries for extraterritorial LI mandates. ICC's February 2012 LI policy statement focuses on this second challenge, recommending that LEAs and governments:
"Improve existing MLATs so that (1) they cover evolving IP-based communications services, (2) they deliver requested data in time frames satisfactory for LEAs, (3) [they] increase legal certainty for compliance with respective national laws; and (4) all multinational service providers know how to interact with the MLAT process (e.g. via efficient, transparent processes and availability of information on that process)."

The policy statement also suggests that "MLAT improvements would advance cross-border law enforcement cooperation, reduce conflict of law difficulties, and reduce the risk of countries establishing unnecessary data-related infrastructure localization requirements."

The present policy statement substantially expands on these earlier ICC recommendations and analysis, based on a careful examination of existing MLATs and associated policy issues. Section II of this statement explains how MLATs work, and the shortcomings of existing MLATs; Section III explains the policy rationale for MLAT improvement; and Section IV contains ten specific recommendations for improvement of MLATs and similar LEA cooperation arrangements. Appendix 1 contains a list of selected MLATs, and Appendix 2 provides a model framework for MLATs and similar arrangements.

II. How MLATs Work and Opportunities for Improvement

MLATs are treaties between two or more countries that define processes and timelines for law enforcement cooperation. Typically, an MLAT addresses some or all of the following points:

- **Parties**
  MLATs can be bilateral (addressing cooperation between LEAs of two countries) or multilateral (addressing cooperation among LEAs of a group of countries). There are also hybrid models – for example, the EU-US MLAT applies to the relationship of each EU member state with a single other country (the United States), and the UN Model Treaty for Mutual Assistance in Criminal Matters is a multilateral model for bilateral MLATs.

- **Jurisdictional scope**
  - A MLAT defines which territories, which types of criminal activity, and which types of judicial proceedings fall within its scope. Application to terrorism and similar borderless criminal activity can be particularly challenging and important.
  - MLATs specify which types of requested assistance must be provided, and which may be refused.
  - A MLAT may also specify its interaction with other treaties (for example where a multilateral MLAT co-exists with bilateral MLATs between parties to the multilateral treaty) and whether the treaty or national law will prevail in the event of conflict.

- **Process for assistance requests**
  MLATs address various procedural issues for legal assistance requests, including the proper form of an assistance request, the authorities from and to which it may be sent and the timing for response.

Some MLATs also explicitly provide for cooperation between LEAs outside formal MLAT processes; however, this is usually described at a very high level, without detail on the process.

- **Details of assistance**
  Descriptions of specific types of legal assistance define the substantive scope of a MLAT, and include one or more of the following:
  - **Documents** may be transferred, including legal process and documentary evidence for judicial proceedings and investigations, sometimes with detailed provisions for particular types of evidence (e.g. banking information);
  - **Testimony** may be taken, both in person and electronically (e.g. via telephone or videoconference);
  - **Interception of electronic communications** may include both communications content and communications data (for example, Government A requesting cooperation from Government B for access to LI-related information that is stored by a private CSP operating in the jurisdiction of Government B), and some MLATs specifically provide for cooperation with private CSPs and/or direct interception by authorities of one country on the territory of another[1];
  - **Cooperative investigations** may involve authorities of more than one country, including by joint investigative teams and by authorities of one country conducting investigations (including covert investigations) on behalf of another country; and
  - Other assistance can include transfer of persons to give evidence in judicial proceedings[2], restitution of criminal property, or "controlled deliveries" of drugs and other contraband.

- **Confidentiality and data protection**
  MLATs often include provisions on confidentiality of the information transferred (although the need for use in judicial proceedings places practical limits on confidentiality), and some MLATs protect individual rights regarding processing of transferred personal data.

- **Costs**
  Some MLATs address the allocation of costs of assistance between the requesting and requested country.

- **Accession and entry into force**
  Like most treaties, MLATs include provisions on how a country may join the treaty as a party (which is particularly important in the case of multilateral MLATs), and how the MLAT enters into force.

This overall approach to MLATs does not need fundamental change. And because new MLATs take time to negotiate; existing MLATs will continue to form the backbone of global law enforcement cooperation for many years to come. However, there are clear opportunities to improve the effectiveness of MLAT processes and coverage in important incremental ways that can be implemented in the near term. **The recommendations in this statement address various types of improvements, including the following:**

[1] The main MLAT providing a right to direct interception across borders is the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000) ("EU MLAC"), Art. 20; (Interception of Telecommunications without the technical assistance of Another Member State). http://www.official-documents.gov.uk/document/cm70/7054/7054.pdf. This present ICC paper does not recommend expansion of such rights, rather focusing on improved cross-border assistance between governments.

[2] Transfer of persons for purpose of prosecution is generally handled separately via extradition treaties, and the potential for overlap between the two types of transfers can sometimes be problematic. Article 15 of the UN Model Treaty on Mutual Assistance in Criminal Matters ("UN Model MLAT"), http://www.un.org/documents/ga/res/45/a45r117.htm, for example, seeks to address this issue.

- MLATs do not have sufficient geographic coverage, in terms of the countries (and bilateral / multilateral country relationships) that they cover. There are notable gaps in some regions of the world (e.g. Asia and Africa), particularly with developing countries that did not previously participate in MLATs.
- The details of assistance specified in most MLATs have not kept pace with the rapid evolution of communications services.
- The speed and efficiency of MLAT cooperation processes is often insufficient, particularly in the context of investigation of Internet-based criminal activity – which typically involves conduct across borders, with criminals having the ability to alter the "location" of their activities extremely rapidly.
- MLATs need to be supplemented by models for LI best practice. In certain jurisdictions there are MLATs in place, but the absence of a domestic LI framework seriously impairs their usefulness[3].

Although the need to address these shortcomings is reasonably self-evident, the next section explains why change is particularly urgent in the face of the increasing challenges of cross-border LI.

III. Rationale for MLAT Improvement

Improving MLATs can be a "win-win-win" for governments, CSPs and the broader public interest.
For governments and LEAs, better MLAT processes can significantly improve prevention and investigation of crime and terrorism. This is particularly the case for conduct requiring a fast response, such as crime and fraud on the Internet (where perpetrators can cover their tracks very rapidly) and situations involving an imminent threat to life or property. As cyber-attacks and hacking increases in scale and impact, the ability of LEAs to identify perpetrators rapidly is key. For governments seeking inward IT investment, there is also a clear opportunity to enhance the attractiveness of their markets by offering clear and transparent processes to multinational providers of communications and IT services, including those offering cloud-based services[4].
For CSPs, the clarity provided by MLATs can reduce burdens of current and emerging LI regulation, particularly the challenges of inconsistent legal requirements that are discussed in Section I above, and that presently subject companies to conflicts of law. Consistent requirements can also help CSPs respond to LI requests in ways that accelerate access to data for LEAs, including by:

- providing CSPs with clarity on LI requirements, which in turn reduces the real or perceived risk of subsequent legal challenge to a CSP decision to supply data and avoids the need for complex dialogues on legal requirements and processes; and
- allowing CSPs to ensure that they have requisite legal authority to implement existing technical protocols for cross-border LI, such as the proposed European Telecommunications Standards Institute (ETSI) "dynamic triggering" process for mobile wiretaps[5].

These benefits for governments, LEAs and CSPs also link directly to broader public interests, including those of:

- safety and security resulting from more effective law enforcement,
- availability of increasingly crucial communications services at reasonable cost, and

[3] For example, this has been a particular barrier to implementation for MLATs involving India, which lacks a clear domestic framework for LI.
[4] Some jurisdictions (e.g. offshore financial centers) have historically offered lack of transparency as a benefit, but ICC believes that the long-term viability and attractiveness of such offerings is on the wane in an increasingly interconnected world.
[5] ETSI draft Technical Standard TS 102 677. Although this standard would not replace specific national legal obligations, it could be influential in shaping those obligations if implemented in a consistent and widespread manner.

- improved protection of privacy and human rights through transparency and procedural restraints on LEAs.

Two possible concerns regarding MLAT improvement are worth considering. First, a substantial amount of work by governments (in cooperation with CSPs) will be required to negotiate new MLATs and improve existing MLATs. Second, new processes for transferring personal information can raise tensions with privacy and data protection rights under national and trans-national law. Both concerns are extremely important, and can be managed in a responsible manner.

On the first concern, it is well worth expanding and modernizing MLAT processes and the invested efforts on this front over the longer term. Indeed, the need to do so is growing, because requirements for cross-border LI are increasing rapidly due to the ongoing evolution of electronic communications infrastructure and services. This trend started with the explosive growth of the Internet that began in the 1990s, but until fairly recently the vast majority of Internet connections and other high-bandwidth data connections were from fixed locations. Now this is changing due to a convergence of new services that are making such connections and communications largely location-independent and device-independent, a trend that some have called "untethering". Broad categories of services that enable untethering include mobile services, cloud computing, machine-to-machine communications, social media, and similar Internet services; and we remain in the early days of the development of such services. The market will certainly provide huge future innovation both of communications networks – e.g. new devices, new infrastructure, new communications protocols, and ubiquitous availability of bandwidth – and of services that use such networks. This is an environment in which the need for cross-border LI cooperation is increasing, because service providers are increasingly located remotely (and often in different countries) from the individuals and businesses using their services[6].

Some countries have responded to these trends through legal / regulatory changes that seek to confine the circumstances in which cross-border LI is required. In particular, some countries have recently mandated that CSPs (whether traditional telecommunications companies, content providers or equipment providers) establish local servers to assist with potential LEA needs. In most circumstances, this is not an appropriate or necessary solution. It puts undue expense on providers (which is ultimately borne by end users), can deter carriers from operating in countries imposing such requirements (which causes self-inflicted harm to economic development), and fails to eliminate the need for access to data held in a third country (which is an increasing reality of changing communications networks). A much better solution – in terms of effectiveness, promotion of innovation, and cost – is to improve cooperation between governments. MLATs and similar processes are and should remain a primary vehicle for such cooperation.

On the second issue above regarding privacy, the effectiveness of MLATs can be increased while upholding privacy protections and other rights that citizens and legal entities have under their national constitutions and other legislation, and under trans-national law (e.g. the EU Data Protection Directive ad Privacy and Electronic Communications Directive). Indeed, it is an inherent feature of MLATs that they provide access to data that would not otherwise be available in a domestic investigation.[7] However, explicit privacy protections under MLATs are far more likely to protect privacy rights than are the inherently *ad hoc* processes of cross-border LI through extra-territorial orders from individual countries, which may rely on a less transparent and legally robust process. The key is to ensure that MLAT

[6] The trend of untethering also has broader implications for change to traditional approaches to LI. ICC's June 2010 policy statement takes a broader view of such changes and how they should be addressed.

[7] *See, e.g.,* Winston Maxwell and Christopher Wolf, "A Global Reality: Government Access to Data in the Cloud" (Hogan Lovells White Paper, 18 July 2012) ("MLATs … make borders and the physical location of data much less significant barriers to governmental access"; noting that such issues exist globally, in Europe, the United States and elsewhere).

procedures are clear and transparent, with appropriate explicit protection of individual rights. Multilateral MLATs in Europe already include explicit data protection provisions[8], and similar approaches (taking into account the variation in privacy laws around the world) are crucial in any new or evolving MLAT frameworks.

IV. Recommendations

The primary aim of this policy statement is to offer practical recommendations that strike a balance among the needs of governments/LEAs, CSPs and the public interest – consistent with the approach taken in the June 2010 ICC policy statement. The ten recommendations below take a focused approach to reducing the burdens of cross-border LI through MLAT improvement, and are divided into three categories: (A) geographic and substantive scope of MLATs, (B) efficient MLAT procedures and (C) education and transparency.

A. Geographic and Substantive Scope

Recommendations 1-3 address the fundamental point that LEAs of different countries cannot easily cooperate when there is no applicable MLAT between them, or where applicable MLATs do not provide for the type of assistance or cooperation that is needed. These recommendations aim to encourage governments to negotiate new MLATs, and adopt amendments to existing MLATs.

- **Recommendation 1: Countries should expand the geographic coverage of multilateral and bilateral MLATs.**

In order to set priorities for negotiating new or amended MLATs, each country (or group of countries, such as the EU) should designate a government agency responsible for identifying other countries that present greatest needs for frequent and/or high-priority law enforcement cooperation. The lists of countries identified (combined with information on existing MLATs) would provide initial priorities for MLAT negotiations, which would then need to be refined in cooperation with negotiating partners.

In setting negotiating priorities, countries should consider specific apparent needs for additional MLAT coverage – including greater coverage of (a) countries outside the EU and US, (b) regions that are not presently covered by a multilateral MLAT[9] and (c) developing countries. In some cases, there may be opportunities to expand or enhance existing multilateral MLAT frameworks, such as those in the EU[10] and the Americas[11].

- **Recommendation 2: MLATs should explicitly cover modes of communication associated with evolving networks and services.**

As explained above, the evolution of networks and services (including untethered communications and machine-to-machine communications) are presenting major challenges for cross-border LI. Some existing MLATs do address cross-border LI involving electronic communications. For example, the multilateral EU Convention on Mutual Legal Assistance in Criminal Matters (adopted in 2000) contains

[8] *See* ("EU MLAC"), Art. 23 (personal data protection); European Convention on Mutual Assistance in Criminal Matters (1959) ("European MLAC"), second protocol, Art. 26 (data protection), http://conventions.coe.int/Treaty/en/Treaties/html/030.htm.
[9] The Asia-Pacific and African regions are notable candidates. The former is an issue that organizations such as the Asia-Pacific Economic Cooperation might consider prioritizing.
[10] *See* EU MLAC; European MLAC.
[11] *See* Inter-American Convention on Mutual Assistance in Criminal Matters (1992), http://www.oas.org/juridico/english/treaties/a-55.html.

detailed provisions on interception of telecommunications[12], including for the situations where (a) an LEA in an EU member state requires access to facilities located in another member state in order to access communications to/from the first member state[13] or (b) an LEA is able to access facilities in its own member state to intercept communications to/from a "telecommunications address" (e.g. a telephone number or IP address) in another member state[14].

New and amended MLATs (*see* Recommendation 1) should take approaches like these. Furthermore, such approaches can be improved through more careful attention to emerging issues such as treatment of (a) users of mobile phones and similar devices while roaming, (b) global Internet content providers whose facilities are primarily located in one or a few countries, (c) cloud computing data stored on behalf of a multinational enterprise. Such situations often defy neat jurisdictional solutions, and further work on appropriate rules for these situations can reduce uncertainty and improve cooperation for LEAs and CSPs. MLAT rules should also ensure proportionality of obligations on providers with limited relevance for LI purposes (e.g. those serving only enterprise closed user groups or having limited business in a given country[15]). Defining such rules should be the subject of further work (including under Recommendation 3).

- **Recommendation 3: Appropriate international and national organizations should cooperate to develop a model MLAT framework and seek to deploy it.**

In 1990, the United Nations adopted the Model Treaty on Mutual Assistance in Criminal Matters[16]. This model treaty is a useful document, but it needs to be updated, including because it does not address the huge changes in communications services in the more than two decades since it was adopted, and related emerging challenges of cross-border LI. Accordingly, the UN and/or other appropriate international organizations, in cooperation with representatives of national governments, should develop a new model MLAT and seek to deploy it widely. The model should be simple enough to encourage widespread adoption, yet effective for the most important forms of cooperation. Furthermore, the model should be flexible enough to accommodate a variety of cooperation scenarios, including for example (1) provision for both bilateral and multilateral cooperation, (2) optional clauses or protocols providing additional details on particular types of assistance, and (3) an approach to transparent cooperation outside of formal MLAT processes. The ICC Commission on the Digital Economy would welcome the opportunity to be involved in development of such a model MLAT framework, and offers an initial outline and approach in Appendix 2.

B. Efficient Procedures

Recommendations 4-8 seek to make MLAT processes as efficient as possible, without compromising individual rights. Efficiency of process is a primary reason that MLATs are an attractive alternative to other means of cross-border LI procedure, including for time-sensitive LEA investigations. Elaborating such changes to MLAT procedures will require a cooperative effort by governments, LEAs and CSPs. Substantial work has been done in various fora (including ETSI) on types of LI data and the best means of transferring such data between LEAs. Appendix 2 contains some further initial ideas for

[12] *See* e.g. EU MLAC, Title III (Art. 17-22).
[13] EU MLAC, Art. 19 (requiring the member state where the facilities are located to designate service providers for providing LI access to those facilities).
[14] EU MLAC, Art. 20 (requiring notification to the member state with which the telecommunications address is associated).
[15] *See* June 2010 ICC policy statement, Recommendations 2 (CSPs serving enterprise customers) and 3 (CSPs with limited business in a given country).
[16] UN Model Treaty on Mutual Assistance in Criminal Matters (1990) ("UN MLAT"), http://www.un.org/documents/ga/res/45/a45r117.htm.

implementation of the recommendations in this section, including the crucial role of LI standards.

- **Recommendation 4: MLATs should include explicit timetables for cooperation and response, both by government and CSPs.**

Explicit timetables for MLAT responses have a dual function. On the one hand, they ensure that the MLAT process is prompt enough for investigatory and judicial needs. On the other hand, they set expectations for response times, ensuring that LEAs and CSPs can design and implement internal MLAT response procedures that both meet the timetables and ensure that other interests (including individual privacy, human rights and cost/proportionality) are protected. Thus, CSPs should be engaged to ensure that any timetables are workable from industry's perspective. MLAT timetables should recognize that CSPs need reasonable time to implement an LI demand once it has been approved by an LEA or other government body through MLAT procedures. MLAT timetables also need to differ for different types of assistance, and for urgent cases.

- **Recommendation 5: MLATs should include a simple process for exchange of essential data for identifying the source/destination of communications across modern networks and services, to allow rapid location of devices and individuals.**

In an environment of untethered communications, one of the biggest challenges for LI and LEAs is that of locating and identifying individuals, devices and data across globally-distributed communications networks. This is a particular problem because devices and data can move or disappear extremely quickly, generally leaving few bread crumbs to follow. To deal with this challenge, MLATs should include expedited processes (with reduced timetables and simplified procedures) for LEAs to exchange essential data for identifying the source and destination of communications. In order to prevent misuse of these processes (and to avoid associated infringement of individual rights), the applicable MLAT provisions should define with specificity the circumstances in which the processes may be used and the types of data that may be exchanged.

- **Recommendation 6: LEAs and CSPs should be required to establish contact points for LI requests.**

It is already a common practice for LEAs and CSPs to establish “single points of contact” (SPOCs) for requests related to LI and other legal process. The use of SPOCs improves efficiency by reducing confusion about where a request should be sent, and leaving it to the receiving organization to decide how the request should be handled internally (which it almost always knows better than does the

requesting organization). It also allows use of technology to improve efficiency and response times – e.g., the telephone number and/or email address used to contact a SPOC can be routed to different individuals at different times depending upon who is on duty. This practice is clearly appropriate for MLATs, and should become an explicit requirement. MLAT SPOCs should have responsibility for making LI requests (in the case of LEAs), receiving LI requests (in the case of CSPs), and answering questions about LI requests (in both cases).

- **Recommendation 7: MLATs should be explicitly linked to other procedures for LEA cooperation.**

In parallel with the development of MLAT procedures, increased coordination of other national and international LEA cooperation procedures is critical. Many LEAs around the world have established relationships for cooperation outside of MLATs and other official channels. Examples include the international “24/7 network” for law enforcement cooperation founded by the US Federal Bureau of

Investigation[17], and a similar EU initiative to set up a cybercrime network to increase coordination between LEAs and others in certain key areas including organized online fraud, child sexual abuse and cyber attacks[18].

Certain direct LEA cooperation, without a formal governing legal regime, does present challenges of ensuring compliance with applicable legal restraints and individual rights; however, such compliance is certainly possible, and LEA cooperation is a necessary reality of modern law enforcement. Some MLATs already explicitly recognize such "spontaneous" cooperation[19], and this linkage should be extended – both by including such provisions in new and amended MLATs, and by considering ways in which the linkage between MLAT and informal cooperation can be tightened to make both forms of cooperation more effective, while ensuring that the receiving party is clear as to its legal responsibilities in providing information (e.g. under privacy law). For example, this could be addressed through a non-treaty-based cooperation system in parallel to the development of MLAT processes (further detail is provided in Appendix 2).

- **Recommendation 8: MLATs should include explicit rules for allocation and reimbursement of costs of assistance.**

ICC's June 2010 LI policy statement recommended that LI costs should be paid with public funds in order to encourage LEAs to impose proportionate LI requirements (Recommendation 6 of June 2010 policy statement), and that fixed LI costs should be reimbursed directly rather than through intercept-related charges (Recommendation 7 of June 2010 statement). Similar principles should be articulated in MLATs, with the added dimension that costs must be allocated between the requesting and requested country. For example, some MLATs set out a default principle that costs should be borne by the requested country[20], but this may not be an appropriate principle in various circumstances (e.g. in complex investigations where the requesting country has substantial discretion on the desirable scope of assistance requests). In addition, although the process of MLAT negotiation would make imposition of disproportionate costs among participating countries unlikely, as a general matter, MLATs should not seek to place new burdens on CSPs (e.g., fixed build out costs or new fixed LI burdens).

C. Education, Cooperation and Transparency

Recommendations 9 and 10 address the straightforward point that for MLATs to be useful and effective, the entities to which they relate (LEAs, CSPs and others) must be aware of available MLATs and be reasonably familiar with their details.

- **Recommendation 9: Governments should educate LEAs, CSPs and others about MLATs and their terms, and cooperate to implement them effectively.**

---

[17] *See* "Combatting Cyber Crime: Global Network Operates 24/7," http://www.fbi.gov/news/stories/2009/january/fordham_011409.

[18] *See* European Commission, Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre, http://ec.europa.eu/home-affairs/doc_centre/crime/docs/Communication%20-%20European%20Cybercrime%20Centre.pdf. This proposal builds on the Council of Europe Cybercrime Convention, which both establishes substantive rules for criminal offences its parties domestic laws and contains wide ranging obligations on signatories on mutual legal assistance in such matters – including the establishment of a 24/7 network between signatories and a SPOC provision. *See* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. This treaty has more than 30 signatories to date, including the United States as a non-party signatory.

[19] *See e.g.* EU MLAC, Art. 7 (Spontaneous exchange of information); European MLAT, Second Protocol, Art. 11 (Spontaneous information).

[20] *See* UN MLAT, Art. 19.

LEAs, judicial authorities, CSPs, and others who may be involved in MLAT processes should know which MLATs are available for which types of assistance, and when and how MLAT requests are made. Such awareness promotes effective functioning of MLAT processes and avoids improper use of those processes. MLAT education should address the substance, process and contact points (see Recommendation 6) for using MLATs. Means of education might include websites, seminars, direct communication to relevant parties, and others.

Such educational efforts should also extend to cooperation across borders. Mutual engagement between the parties to an MLAT is crucial, and the effectiveness of many MLATs correlates directly with the extent of engagement between the parties to it and the effort devoted to such cooperation – e.g. establishing points of contact, ensuring dialogue among involved governmental bodies, and regular assessment of what is working and what is not.

- **Recommendation 10: ICC should develop a publicly-available, Internet-based catalogue of MLATs and associated resources, for use by CSPs, LEAs and the public.**

This recommendation is self-explanatory. ICC's Commission on the Digital Economy and its member companies would welcome the opportunity to play a role in producing such a catalogue, as improved transparency of such information will aid in the effort to improve MLATs. Such a catalogue can leverage existing work like the OAS Hemispheric Information Exchange Network for Mutual Assistance in Criminal Matters and Extradition[21].

ICC and its members are open to dialogue with LEAs and governments on how these recommendations can best be implemented.

[21] *See* http://www.oas.org/juridico/mla/en/index.html.

Appendix 1 – Selected MLATs

Key multilateral MLATs:

1. European Convention on Mutual Assistance in Criminal Matters (1959), http://conventions.coe.int/Treaty/en/Treaties/html/030.htm
2. UN Model Treaty on Mutual Assistance in Criminal Matters (1990), http://www.un.org/documents/ga/res/45/a45r117.htm
3. Inter-American Convention on Mutual Assistance in Criminal Matters (1992), http://www.oas.org/juridico/english/treaties/a-55.html
4. Economic Community of West African States (ECOWAS), Convention A/P.1/7/92 on Mutual Assistance in Criminal Matters (1992)
5. Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000), http://www.official-documents.gov.uk/document/cm70/7054/7054.pdf (text), http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_criminal_matters/l33108_en.htm (explanation)
6. Council of Europe Convention on Cybercrime (2001), http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Selected bilateral or hybrid MLATs:

7. EU-US MLAT, http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:181:0034:0042:EN:PDF
8. Canada-US, Treaty on mutual legal assistance in criminal matters (1985), http://www.treaty-accord.gc.ca/text-texte.aspx?id=101638
9. UK-US, Treaty on mutual legal assistance in criminal matters (1994), http://www.fco.gov.uk/resources/en/pdf/treaties/TS1/1997/14
10. US-China, Agreement on mutual legal assistance in criminal matters (2000), http://www.state.gov/documents/organization/126977.pdf
11. US-India, Treaty on mutual legal assistance in criminal matters (2001), http://www.glin.gov/view.action?glinID=112915
12. China-Australia, Treaty on mutual legal assistance in criminal matters (2006), http://www.austlii.edu.au/au/other/dfat/nia/2006/38.html
13. List of India MLATs with 30 developed and developing countries, see http://www.cbi.gov.in/interpol/mlats.php

Appendix 2 – Model Framework for MLATs and Similar LEA Cooperation

This appendix provides initial, high-level principles for model MLATs, including bilateral, multilateral and hybrid MLATs, as well as other forms of cooperation among LEAs. Detailed provisions will require substantial additional work, and the Commission on the Digital Economy would welcome the opportunity to participate in this work.

1. **The UN Model Treaty on Mutual Assistance in Criminal Matters ("UN MLAT") provides a good starting point, particularly with respect to traditional MLAT provisions.**

2. **Various additions to the UN MLAT are needed, some of which might be contained in optional clauses or protocols:**

- General scope – consider general, expansive statement of jurisdiction over "offences … within the jurisdiction of the judicial authorities of the requesting State" (UN MLAT, Art. 1(1)) vs. more detailed specification offences (Recommendation 1)

- Coverage of current and evolving communications services (Recommendation 2)
  - Title III (Art. 17-22) of EU MLAC provides initial model for telecommunications LI
  - Services / CSPs to be considered
    - Mobile roaming
    - Cloud computing
    - Global online service providers (e.g. social media)
    - Machine-to-machine communications (fixed and mobile)
  - Explicit technology neutrality
  - Linkage to international standards (e.g., ETSI standard ES 201 671)

- Other expanded scope (Recommendation 3 and Section II above)
  - Restitution of property[22]
  - Banking / financial information[23]
  - Video testimony[24]
  - Controlled deliveries of drugs/contraband[25]

- Explicit response timetables – improve UN MLAT, Art. 6 (Recommendation 4)

- Expedited procedures for source/destination of communications (Recommendation 5)

- Contact points – improve UN MLAT, Art. 3 (Recommendation 6)

- Linkage to other cooperation processes – improve UN MLAT, Art. 2 (Recommendation 7); model cooperation process discussed in point 3 below

- Cost allocation rules – improve UN MLAT, Art. 19 (Recommendation 8).

3. **In addition to an MLAT treaty framework, it would be appropriate for there to be an internationally-agreed Reference Paper for LI cooperation between governments and CSPs**

[22] *See* e.g., EU MLAC, Art. 8.
[23] *See* e.g., EU-US MLAT, Art. 4.
[24] *See* e.g., EU-US MLAT, Art. 6; EU MLAC, Art. 10.
[25] *See* e.g., EU MLAC, Art. 12.

with respect to communications traffic data (but not communications content), which could include the following provisions:

- Definitions
  - "Communication Content", "Handover Interface (HI)", "Handover Interface port 1 (HI1)" and "Handover Interface port 2 (HI2)" have the meanings given in ETSI standard ES 201 671
  - "Telecommunications Data" has the meaning given to "Intercept Related Information" in ETSI standard ES 201 671.

- Scope and objectives
  - Each Signatory Party to the Reference Paper (or Annex, if existing MLAT in place) grants to all other Signatory Parties the widest measure of mutual assistance in the provision of Telecommunications Data in connection with investigations, prosecutions and proceedings related to criminal matters in accordance with the Reference Paper.
  - Scope includes criminal offenses against a law relating to [either (a) tie to definition in existing MLAT or (b) specify particular offenses e.g. taxation, customs duties, foreign exchange control and other revenue matters].
  - The Reference Paper does require any Signatory Party to provide Communication Content.

- Technical interfaces
  - Each Signatory Party will provide one or more handover points for the provision of Telecommunications Data. Each handover point is a Handover Interface port 1. If a Signatory Party provides more than one HI1, it will provide information as to the type of assistance that is available from each HI1.
  - Each Signatory Party will provide one or more Handover Interface port 2. Each Signatory Party shall provide the form in which metadata is delivered at HI2, based on the definitions in the ETSI standard ES 201 671. (The goal over time is to define common metadata exchange standards for emerging technologies, including via evolution of ETSI standard ES 201 671.)

- Response timetables – each Signatory Party will respond within [x] days to acknowledge receipt of a request. Within [x] days, the signatory party will provide the relevant data to the requesting party.

The International Chamber of Commerce (ICC)

ICC is the world business organization, a representative body that speaks with authority on behalf of enterprises from all sectors in every part of the world.

The fundamental mission of ICC is to promote open international trade and investment and help business meet the challenges and opportunities of globalization. Its conviction that trade is a powerful force for peace and prosperity dates from the organization's origins early in the 20th century. The small group of far-sighted business leaders who founded ICC called themselves "the merchants of peace".

ICC has three main activities: rule setting, dispute resolution, and policy advocacy. Because its member companies and associations are themselves engaged in international business, ICC has unrivalled authority in making rules that govern the conduct of business across borders. Although these rules are voluntary, they are observed in countless thousands of transactions every day and have become part of the fabric of international trade.

ICC also provides essential services, foremost among them the ICC International Court of Arbitration, the world's leading arbitral institution. Another service is the World Chambers Federation, ICC's worldwide network of chambers of commerce, fostering interaction and exchange of chamber best practice. ICC also offers specialized training and seminars and is an industry-leading publisher of practical and educational reference tools for international business, banking and arbitration.

Business leaders and experts drawn from the ICC membership establish the business stance on broad issues of trade and investment policy as well as on relevant technical subjects. These include anti-corruption, banking, the digital economy, marketing ethics, environment and energy, competition policy and intellectual property, among others.

ICC works closely with the United Nations, the World Trade Organization and intergovernmental forums including the G20.

ICC was founded in 1919. Today it groups hundreds of thousands of member companies and associations from over 120 countries. National committees work with ICC members in their countries to address their concerns and convey to their governments the business views formulated by ICC.

ICC Commission on the Digital Economy

Business leaders and experts develop and promote the continued and stable growth of the Digital Economy, and further adoption of its underlying ICT foundation, through regulatory advocacy of key business positions and best practices through ICC's Commission on the Digital Economy.

Through its members who are ICT users and providers from both developed and developing countries, ICC is recognized in expert circles as the global consensus voice for private sector expertise on policy matters that drive the Digital Economy. It also provides the ideal platform for developing global voluntary rules and best practices for this area of interest to companies worldwide. Dedicated to the expansion of secure ICT-facilitated trade, ICC champions the liberalization and regulatory harmonization that are required to achieve a free flow of information across all borders.

ICC led and coordinated the input of business around the world to the United Nations World Summit on the Information Society (WSIS), Geneva 2003, Tunis 2005, and continues this effort in the activities established in the Tunis Agenda through its initiative, Business Action to Support the Information Society (BASIS http://www.iccwbo.org/basis).

International Chamber of Commerce
The world business organization
Policy and Business Practices
38 Cours Albert 1er, 75008 Paris, France
Tel +33 (0)1 49 53 28 28 Fax +33 (0)1 49 53 28 59
E-mail icc@iccwbo.org Website www.iccwbo.org