Lee-Makiyama, Hosuk

Research Report

A multilateral legal assistance protocol: Preventing fragmentation and re-territorialisation of the internet

ECIPE Policy Brief, No. 9/2013

Provided in Cooperation with:
European Centre for International Political Economy (ECIPE), Brussels

Suggested Citation: Lee-Makiyama, Hosuk (2013) : A multilateral legal assistance protocol: Preventing fragmentation and re-territorialisation of the internet, ECIPE Policy Brief, No. 9/2013, European Centre for International Political Economy (ECIPE), Brussels

This Version is available at:
https://hdl.handle.net/10419/174780

POLICY BRIEFS
No. 09/2013
ISSN 1653-8994

A Multilateral Legal Assistance Protocol: Preventing Fragmentation and Re-territorialisation of the Internet

Hosuk Lee-Makiyama *Hosuk Lee-Makiyama (hosuk.lee-makiyama@ecipe.org) is Director of ECIPE*

Few aspects of the modern legal debate are as controversial and engaging for the general public as the regulation of the Internet. It is routinely assumed that the inherent transnational nature of the Internet represents the biggest challenge to national jurisdictions. Minus the added alarmism, it is not an incorrect assumption. For instance, the total number of jurisdictions involved in the simplest e-commerce transaction is overwhelming: the customer, the seller's legal entity and its physical servers could be placed in three different jurisdictions. And the physical delivery and financial payment of the purchase could be separated from the process and handled from additional locations and jurisdictions. Most cases of cross-border transactions online (or subsequent disputes when they have occurred) are matters of commercial law and international private law. Thanks to the contractual relationship between the private parties, most transactions are, at least in practice, less complex or common than they were envisaged to be. Other aspects of law, like criminal law or tort law, require state involvement and are not easily settled.

Online crime that originates in foreign jurisdictions has emerged as one of the legal problems in the interconnected nature of the new internet-driven economy.

SUMMARY

This paper addresses the question of legal cooperation and enforcement regarding online crime. It shows how ineffectual legal-assistance cooperation increasingly prompts governments to apply laws extraterritorially or to force re-territorialisation requirements on business, with consequences for the free flow of data and the global economy. Finally, the paper outlines ideas for the improvement of legal assistance, especially through a new Multilateral Legal Assistance Protocol.

The paper highlights the issues that arise when several different layers of national laws counteract and sometimes contradict one another. Governments often seek to impose their laws outside their territories, or even try to physically prevent users and businesses from falling under the jurisdiction of other countries. In response, governments have also sought to conclude bilateral and multilateral treaties in judiciary and commercial cooperation, most notably free trade agreements (FTAs). Mutual legal assistance treaties (MLATs) or international binding treaties, such as the Council of Europe's Convention on Cybercrime, would have to be revised or augmented to address the problems of online criminality while making some of the disproportionate examples of extraterritorial and unilateral measures unnecessary through international cooperation.

An alternative – or, for some, complementary – approach is for countries to establish a new Multilateral Legal Assistance Protocol (MLAP). This Protocol would lay down stricter standards for legal assistance cooperation and build in stronger safeguards to ensure that legal assistance protects civil liberties, human rights, rule of law and core principles of transparency. Finally, the Protocol would provide negative rules to prevent governments from re-territorialising data.

The Internet has enabled various forms of fraudulent acts that take place across borders. Such incidents often involve the dissemination of universally forbidden products that, like the rest of society, have simply moved online, e.g. child pornography. But there are also examples of crimes that are less straightforward or obvious. For example, a blog post considered legal and harmless in the provider's country but may be illegal due to its political content, or constitute libel or a hate crime in other jurisdictions. Countries may apply different interpretations to the protection of free expression – yet most items online are immediately and universally available. Similarly, some services, such as gambling, alcohol or pornography, may be legal activities in some countries while subject to government monopoly or even criminalised in others.

This conflict is not new. Similar difficulties in reconciling law and technology occurred with the arrival of the printing press, shortwave radio and satellite broadcasting. But some issues are entirely novel and unique to the Internet. For example, the Internet creates an aggregation of 'big data' of customer behaviour that is routinely monetised for e-commerce and advertising, which has raised some concerns about possible privacy violations, especially in the light of recent revelations about global electronic surveillance in which many major telecom and internet services were accomplices. The importance of intermediaries in digital commerce complicates the situation still further. Online streaming, blogs, search engines, email or booking agents are merely platforms that may be unaware of what their users publish, or unable to be held fully accountable for content. They may also be based in a different country to the other links in the supply chain.

Is it possible for policymakers to address growing concerns about online crime in multiple jurisdictions? This paper argues that there is a solid case to improve current legal cooperation on online crime. It is a far better – and simpler – option than what now appears to be the alternative: countries resorting to policies that apply laws extraterritorially or that demand re-territorialisation of data in order to improve the effectiveness of law enforcement – or countries seeking to physically prevent users and businesses from falling under the jurisdiction of other countries. Some governments have sought to conclude bilateral and multilateral treaties in judiciary and commercial cooperation, most notably free trade agreements (FTAs). Mutual legal assistance treaties (MLATs) or international binding treaties, such as the Council of Europe's Convention on Cybercrime, are other tracks followed by governments. This paper argues that several approaches are needed to improve cooperation in law enforcement. At the centre should be a plurilateral approach, based on the principles of Council of Europe's Convention of Cybercrime. An important addition, however, is that such an agreement or protocol, or in complementary agreements, prevents countries from imposing localisation requirements on data operators and providers. Law enforcement cooperation that reinforces current trends of Internet fragmentation should be avoided.

EXTRATERRITORIALITY – THE LAW OF THE LAND OR THE JUNGLE?

Many existing regulations governing activities on the Internet were enacted in the pre-Internet era, and the rise of the Internet has inarguably necessitated a modernisation of certain classic legal concepts and instruments. One conflict – between the global nature of the Internet and the territorial nature of law – has been accelerating in recent years. It has led to disputes between different state jurisdictions, producing inconsistent results or double jeopardy. This is the result of extraterritoriality – the practice of applying national laws beyond their territorial limits – leading to a conflict between generally undesirable laws.

To avoid conflict of forums, almost all legal systems contain rules on whether their law should apply in transnational felonies committed in part outside their natural jurisdiction. These forum rules are sometimes conflicting, and two legal systems could claim jurisdiction over a case concerning a felony committed online. Most jurisdictions apply the principle of territoriality, i.e. where the offence physically took place – but as outlined in the introduction, 'place' is often ambiguous and indistinct on the Internet, and different legal systems and case laws offer different solutions. These problems are not a new phenomenon. Principles of maritime law were developed over a thousand years as customary law, and solved the issue by extending a nation's jurisdiction to its vessels. As

a result, the high seas are not lawless lands and murderers on ocean liners in Agatha Christie novels did not walk free. Some acts, such as naval piracy or crimes against the humanity, are considered so heinous that any jurisdiction should intervene regardless of territorial jurisdictions – a so-called erga omnes obligation.

However, the Internet is not the high seas, and the vast majority of internet crimes would not qualify as crimes against humanity. The real problem is rather that the Internet has become subject to a myriad of overlapping jurisdictions and conflicting obligations. Domestic laws are routinely enforced extraterritorially on online activities originating from or taking place abroad. The Internet is far from the lawless land it is claimed to be. The most common argument for extraterritorial application is based on nationality, i.e. the perpetrator is a citizen of the country. To a certain degree, this follows basic logic – it is likely that the defendant and its assets are located in its home jurisdiction, which would facilitate investigation, securing of evidence and eventual enforcement of sanctions.

In other cases, the principle of passive personality applies, where the law of the injured seeks jurisdiction on the matter. Cases involving environmental law where the source of pollution affecting a jurisdiction comes from another country are a classic example. For example, the EU has been criticised for the emission charges it levies on foreign airlines which it calculates from the point of departure, including the distance flown over non-EU territories.

As noble as these objectives may seem, an extraterritorial imposition of one country's law over another jurisdiction is controversial. Take for instance the case of Yahoo v LICRA, one of the first cases concerning internet extraterritoriality. Yahoo was charged with promoting Nazism in France (where it held no servers or operational assets) when its services were used to host an online auction of Second World War memorabilia. The auction was not explicitly aimed at French users, but nonetheless available for all.[1] While displaying such items is illegal in France, blocking the sale contravenes free speech under the First Amendment in the US constitution – and US courts initially had to consider whether the French ruling could be enforced in the US. Another case of French–US conflict of jurisdiction concerned a US-based video streaming service broadcasting a fashion show where certain logotypes were prominently displayed in a manner that violated French copyright laws,[2] but may have been covered by the concept of fair use under US laws.

TERRITORIALISATION AND BALKANISATION

In the case against Yahoo the French court argued that the firm could have simply excluded almost all French users by blocking certain IP addresses from accessing the relevant pages. However, no business or publisher could possibly foresee or oversee the legality and compliance of their activities according to every legal system where their web page can be viewed.

In contrast, some countries go to some extraordinary lengths to avoid extraterritorial application. Paradoxically, such endeavours only produce remarkably similar outcomes. China, for example, applies a notification system at home against inappropriate content in its jurisdiction. This system is not extended to non-Chinese websites as they are deemed to lie outside mainland China's jurisdiction. Instead, China blocks or filters thousands of foreign web sites outside its territory (through the so-called Great Firewall of China or Golden Shield, depending on what your politics are). An internet service provider would need to apply for a domestic internet content provider (ICP) licence, and must de facto come under Chinese jurisdiction according to the territorial principle in order to be guaranteed access to the Chinese public.

The balkanisation and nationalisation of the Internet continues, especially in the wake of recent revelations of alleged electronic surveillance programs. Many of the policy responses by affected countries deliberately disrupt open data flows or clearly work to that effect. For example, a full-scale data localisation requirement was also proposed in Brazil in 2011 and its legislative process was

1. Yahoo v LICRA, TGI de Paris, 2000

2. Sarl Louis Ferarud v Viewfinder, 489 F 3d 474, New York, 2007

expedited by the revelation that the Prism program was targeting the country.[3] The proposed General Data Privacy Regulation (GDPR) in the EU contains many problematic aspects[4], and one of the most serious flaws concerns the prohibition on moving and processing data freely in and out of Europe unless the processing takes place in a jurisdiction that has based its laws on the EU regulation or uses it as a template – regardless of whether it is actually an adequately safe legal environment.[5] Malaysia and Russia have also implemented a similar model of privacy regulation which prohibits the transfer of personal data abroad by default.[6] Korea has proposed similar measures in the financial sector despite undertaking commitments to open the cross-border flow of data in their recent free trade agreements (FTAs) with the EU and the US.

Data localisation requirements are damaging the open-ended nature of the Internet, especially when its proponents include democracies. It disrupts the free flow of information and entails huge costs for domestic as well as foreign holders of data that want to transport data in and out of countries for perfectly legitimate purposes. Data localisation requirement fragments the Internet into national enclosures where only the home-grown fauna is allowed to play. Traditional manufacturing and services sectors are also increasingly dependent on data processing as their most important source of input, often exceeding the importance of raw materials or labour costs. Thus forced data localisation comes at extremely high costs in lost competitiveness and productivity.[7]

3. Marco Civil da Internet, PL 2126/2011; See also speech delivered by President Rousseff to the 68th Session of the UNGA, on September 24th, 2013
4. European Commission, COM(2012)11, January 25th, 2012
5. See Bauer, Erixon, Krol, Lee-Makiyama, 2013
6. Blackmer, W. Scott, Transborder data flows at risk, Information Law Group, accessed from: http://www.infolawgroup.com/2012/02/articles/cloud-computing-1/transborder-data-flows-at-risk/
7. Lee-Makiyama, European leaders should leave data flows open, Euractiv, September 30th, 2013, accessed from: http://www.euractiv.com/infosociety/european-leaders-leave-data-flow-analysis-530785

ONE SINGULAR LAW FOR THE INTERNET?

Twenty years into the Internet era, some of the early utopian notions of the Internet being disconnected from the rules of the physical world are impractical, or perhaps even inane. In fact, few today preach the principle of internet exceptionalism.[8] Exceptionalists have two modern incarnations: those who advocate a digital libertarian playground and, often sailing under a different flag, those who wish to impose higher levels of liability or responsibility online than on equivalent actions offline on the grounds that the Internet is *different* and somehow exceptional. Such views only help to marginalise the Internet, which in turn legitimises further balkanisation. Instead, the existence of the Internet as an open network depends on functioning legal frameworks, global and domestic. A proportionate legal prescription, followed by effective enforcement is an essential prerequisite for the Internet to exist in its current form, to avoid conflict of laws and balkanisation.

To solve the extraterritoriality problem and internet balkanisation, it is necessary to investigate why domestic laws are applied to other territories for internet-related crimes in the first place – and for the sake of the discussion, let us ignore the political incentives for populist crackdowns on the Internet in the name of winning elections. The fundamental and underlying rationale for legislatures and courts to seek to apply their laws to others is simply deeming their laws to be better than – or at least different to – those of other jurisdictions. Standards and obligations, such as sales tax rates, are almost always different or have different beneficiaries. Some legal concepts (e.g. free speech or fair use) and their caveats are interpreted differently. Others, like the ban on Nazi memorabilia, are unique characteristics of one particular system and do not exist in others. Under such circumstances, the remedy sought cannot be offered by applying the other parties' legal system.

Such regulatory divergences are usually addressed through international cooperation, regulatory harmonisation and the setting of common standards. Even in the most advanced form of pooled sovereignty and

8. See Wu, Tim, Is Internet exceptionalism dead?, TechFreedom, 2010

law-making – namely the EU and its Single Market – the design of common supranational rules for the Internet has been an unwieldy affair: criminal law and sanctions are still the competences of its individual Member States. To date, all major pieces of legislation concerning the Internet were directives (under which the implementation is left to the individual Member State) rather than union-wide regulations.[9] The disagreements over the proposed General Data Privacy Regulation in the EU proves that effective legal harmonisation is difficult to accomplish, even amongst a relatively small group of economically and culturally homogeneous countries.

INTERNATIONAL WORK ON INTERNET LEGAL PRESCRIPTION

Regulatory harmonisation through legal prescription is evidently difficult to achieve. Some international organisations like the OECD have issued non-binding guidelines and recommendations.[10] Only a few treaties exist in the World Intellectual Property Organization (WIPO)[11] and the World Trade Organization (WTO).[12] Arguably, the most successful forum for legal harmonisation has been the WTO – its members successfully challenged the US ban on online gambling and Chinese restrictions on online movies and music, and it managed to do so through a dynamic and analogous interpretation of decades-old rules on trade in services, rather than new rules developed for online commerce.[13]

Bilateral free trade agreements (FTAs) or regional trade agreements (RTAs) offer a more flexible setting with fewer counterparts than the WTO or the WIPO. However, while FTAs have been precise on traditional matters of trade agreements (tariffs and rights of establishment), the language on rules and regulatory cooperation is often deliberately written in an ambiguous fashion designed to bind its counterparts (i.e. states), and not necessarily to be enforced (i.e. bind its citizens). A critique of trade law derives from the common misunderstanding that it should be read or interpreted as civil law, and not as the instrument of a political compromise negotiated between two or several parties to express a common intention to refrain from protectionist and discriminatory measures. Most provisions in trade agreements are based on the principle of negative liberalisation – i.e. by requiring its signatories to refrain from imposing trade barriers and introducing discriminatory practices –rather than positive law with provisions that have direct binding effect as national law. This kind of drafting technique is not entirely without merit – next generation FTAs and RTAs (e.g. the Trans-Pacific Partnership and the EU–US Transatlantic Trade and Investment Partnership) are expected to contain language that would effectively restrict the signatory governments from requirements such as local data localisation, use of local infrastructure or establishment of local presence. Similarly, both EU and US FTAs could prohibit laws that block transferring information, accessing public or proprietary information stored in other countries.

COOPERATION ON ENFORCEMENT

Finally, there is the other half of the exercise of jurisdictions, namely enforcement. Law enforcement collaboration has, historically, been captured in mutual legal assistance treaties (MLATs).[14] These treaties outline rules and regulations for the exchange of information, for collaboration and the execution of orders between courts and law enforcement agencies. MLATs often specify the necessary criteria required for a request from one country's law enforcement to be honoured, and are widely disseminated. The US, for instance, has entered into more than 60 bilateral MLATs, and even a simpler agreement (MLAA) with China.

9. See e.g. E-Commerce Directive, 2000/12/EC; Directive on privacy and electronic communications, 2002/58/EC
10. OECD Council Recommendation on Principles for Internet Policy Making, 2011
11. So-called 'Internet treaties' consisting of the WIPO Copyright Treaty (WCT) and the WIPO Performance and Phonogram Treaty (WPPT).
12. Notably the General Agreement on Trade in Services (GATS) with its annex and reference papers and the E-Commerce Moratorium.
13. WTO, U – Online Gambling (DS285); China – Publications and Audiovisual Products (DS363)
14. It should be noted that members of the EU have agreed on a framework with the effect of simplifying the rules on exchange of information and intelligence between law enforcement agencies in the so-called 'Swedish Initiative' of 2006. For further information, see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:386:0089:0100:EN:PDF

However, enforcement cooperation takes place between two countries without MLATs. Most countries respond to legitimate requests from foreign courts or via diplomatic channels even in the absence of a MLAT. Some countries require dual criminality, i.e. the act must be an offence in both jurisdictions, while some countries, such as France, Italy and others have caveats for situations in which granting the request could threaten the public order or national interests. Others (e.g. Japan, Russia and Spain) provide mutual legal assistance regardless of whether a treaty exists, provided that the requesting party offers a 'guarantee' (or, perhaps, IOU) that they will reciprocate when they make the same sort of request in the future.

In addition to bilateral and regional MLATs, many UN conventions on transnational organised crime, bribery, narcotics or money laundering provide a basis for mutual legal assistance between the signatories. Although several initiatives by various international organisations have sought to address the issue of online crime,[15] only one treaty is actually in force: the Convention on Cybercrime at the Council of Europe (CoE).[16]

To date, 51 countries are signatories (in some cases awaiting ratification), including several large non-CoE countries like the US, Japan, Canada and Australia.[17] The treaty works as a common standard and provides a definition of activities that must be criminal offences under national law.[18] Jurisdiction is clearly in accordance with the territory principle, supplemented by the nationality principle only when 'the offence is committed outside the territorial jurisdiction of any State'.[19] Furthermore, it requires that any sanction must be 'proportionate' to the crime. Its application is also safeguarded by caveats for human rights, fundamental freedoms, civil and political rights and the principle of proportionality.[20] Under the Convention on Cybercrime, there are also binding rules on extradition, expedited preservation and collection of data (to be shared partially with the requesting party and only to the extent it is necessary) besides the normal course of mutual legal assistance.

Although the Convention on Cybercrime is an ambitious endeavour, there is no shortage of criticism against it. Like many international treaties that are results of lengthy negotiations, its language is sweeping, unspecific and dependent on the good faith of the signatory. For example, certain common commercial practices such as 'cookies' (that places a small file on a user's device without explicit consent) could be interpreted in bad faith as illegal hacking; the scope of the convention could be construed as not addressing cyber crime, and just electronic evidence gathering for all types of crimes which raises particular concerns given that signatories must enact laws that would force service providers to collect or surrender user data, even in real-time. This may already be a common practice in modern law enforcement, but becomes particularly problematic as the convention have no explicit means to safeguard proportionality and balance between the alleged crime and surveillance undertaken by the law enforcement agencies.

The Convention is also open for ratification by more or less oppressive governments who could, at least in theory, request co-operation. The convention prescribes that certain acts that must be deemed criminal (i.e. legal harmonisation) rather than prescribing a strict dual criminality principle (convention only applied when the act is criminal in both countries). As a result, there is a possibility that the convention could force a country to collect evidence on an activity although the act is not a crime in there – or simply have a different views on whether the requested surveillance is proportionate to the felony investigated.

There are also other cultural and constitutional differences amongst the signatories – some countries apply capital punishment, which other consider to be a caveat from extradition and other forms of legal co-operation on humanitarian grounds; the constitutional structure of some

15. cf. United Nations Congress on Crime Prevention and Criminal Justice, Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime: Working paper prepared by the Secretariat, 22 January, 2010
16. Council of Europe, Convention on Cybercrime, CETS No. 185, 23/11/2001. Also referred to as the Budapest Convention.
17. Per September 2013
18. Defined activities are illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to copyright.
19. Art 22.d
20. Art 15.1

countries prohibits its federal level to interfere with its state entities on matters relating to criminal or penal law - international treaties (concluded by a federal government) do not always bind states, regions or provinces in such cases; also, the Convention also requires each party to establish extraterritorial jurisdiction on vessels flying its flags, while some legal systems (e.g. the US) do not automatically do so.

A COMPREHENSIVE FRAMEWORK: THE MULTILATERAL LEGAL ASSISTANCE PROTOCOL (MLAP)

Critics conclude there is a need to reform the Convention on Cybercrime – another alternative is to consolidate the various international frameworks on legal assistance, trade and human rights into a new comprehensive framework, even if such reforms will demand a complicated renegotiation. MLATs, court orders or international conventions are all instruments that could be used as a basis for legal assistance requests. However, the actual underlying mechanism of legal assistance (where a country acts on behalf of the criminal law system of another country) pre-dates the Internet, and is not designed for the globalised reality in which criminal activities disseminate online as easily as an email. The experience of assistance requests shows that the case-by-case process of individual requests is cumbersome and time consuming. Processing times may vary, but often exceed six months.

The language in MLATs and international treaties is ambiguous, and the forms and procedures of 'expedient' collaboration (e.g. deadlines, notification times) are not specified. This leads to situations where mere formal flaws in requests result in extended lead times that often hamper the ability of law enforcement agencies to investigate crimes in the digital environment. Such inefficiencies simply defeat the purpose of the provisions on data preservation and collection of data that exists in the Convention on Cybercrime – in a world where crime is moving as quickly as bits, such lags inevitably mean that the criminals can erase data, change their patterns, and disappear easily before any data is exchanged between the two legal systems. The International Chamber of Commerce has called for reforms and suggested measures ranging from using electronic communication to setting out guidelines for the application of treaty obligations in a way that would possibly shorten the handling times.[21]

The separation of legal prescription, standards, rules on jurisdiction and commitment on enforcement creates a discord and asymmetry of commitments. For example, a contracting party to the Convention on Cybercrime could live up to all of its elements and still enforce rules on forced data localisation or prohibit access to legitimate data on servers abroad. In theory, a signatory of the convention should not need defensive tools against other parties.

It is clear that there is a need to reform and consolidate the existing systems, even if such reforms will demand a complicated renegotiation. Given current trends – where countries are increasingly substituting mutual law enforcement assistance with regulations forcing localisation of data – it is difficult to see why it would be in some countries' interest to deepen law enforcement assistance. The solution is to marry the legal and economic objectives with each other: improved law enforcement assistance removes the only legitimate argument for countries to demand greater access to data through localisation rules. Arguably, the key to reform is the capacity of countries to conclude interdisciplinary agreements that combine or hinge effective legal assistance with internet freedoms that bring economic and general political value. This conditionality unlocks benefits, legal certainty and the effective prosecution of online crime in a way that the current web of agreements cannot.

One possible context for such an exercise is FTA talks. The EU, for instance, routinely demands that its trade partners sign political Partnership and Cooperation Agreements (PCA), where the contracting parties commit themselves to a list of principles and cooperations in areas such as energy, research, social issues, justice and home affairs. In effect, being a signatory to a number of international treaties on human rights is already a precondition for concluding an FTA with the EU.

21. International Chamber of Commerce, ICC policy statement on Using Mutual Legal Assistance Treaties (MLATs) To Improve Cross-Border Lawful Intercept Procedures, No. 373/512m 12 September 2012,

TABLE 1: THE THREE PILLARS OF THE MULTILATERAL LEGAL ASSISTANCE PROTOCOL

LEGAL ASSISTANCE	SAFEGUARDS	LOCALISATION RULES
• National authority responsible for processing requests for assistance • Rules on notification by requesting authority • Rules on notification to domestic authority • Rules (time limits) on veto of request • Rules on time to process request	• Protection of human rights and civil liberties • Quality of institutions to protect human rights and civil liberties • Rule of law and the right to appeal • Transparency in the execution of law enforcement requests • Rule on liability	• Negative rules on regulations with the intent or effect of localising data to a specific jurisdiction • Negative rules on specific and relevant extraterritorial application of law

If the legal co-operation is to be expanded beyond what is stipulated today in the Convention on Crime, the facilitated procedures for legal assistance could be conditioned to a ban on unilateral restrictions and extraterritorial application of their laws on internet activities, as such measures should be no longer required. Furthermore, there must be a reciprocal exchange between minimum legal standards and the expedient processing. In an improved and comprehensive Multilateral Legal Assistance Protocol (MLAP), the need for speed should be balanced with uncompromised safeguard for the rights and liberties of individuals.

Such safeguards in the new system should be higher than those in the existing network of agreements. In return, such a protocol could provide a mechanism that regulates the procedures in which law enforcement agencies request and secure information from private entities and online services providers directly in a participating country. This degree of high-level cooperation would require that signatories have solid legislation on notification, notice and take-down procedures, intermediary liability and unconditional access to an independent process of repeal. As full and effective reciprocity is required, the level of safeguards for proportionality, fundamental rights, human rights, transparency, and the rule of law must be consistent amongst the signatories – and at this stage, the Convention on Cybercrime already contains general principles regarding safeguards, but not on actual procedure or liability. As a result, each country can subjectively decide what a 'proportionate' enforcement actually means.

The envisaged Multilateral Legal Assistance Protocol would build on three pillars.

- The *first pillar* of the MLAP would lay down the standards of law enforcement to which assistance countries commit themselves in this Protocol. Critical elements of this pillar would detail exactly what countries are obliged to do when they receive a request from another signatory. For instance, the time to process a request should be specified. The Protocol should demand that every signatory specifies which entity will be the responsible for handling requests for law enforcement assistance. A negative repeal rule could also form part of the second pillar, stipulating that a domestic entity – e.g. a court or an executive body – with the authority to overturn a request could only do so if they act within a certain (short) time limit. Inevitably, time is of essence. The only way that a new Protocol could generate sufficient confidence in law enforcement assistance is to detail positive and negative rules.

- The *second pillar* of the MLAP would improve on the standards in current treaties and agreements, and would make the principles and safeguards (and the institutions tasked to uphold them) more precise. Principles on civil liberties, human rights and transparency are essential for such an agreement to work. Without them – and without effective domestic systems to guarantee these principles – there will never be enough

trust between countries to allow for the necessary deepening of law enforcement assistance. Likewise, in order to build general trust for the operation of law enforcement agencies and their requests to foreign agencies, there should be systems of reporting and accountability that allow better public scrutiny of whether the rule of law has been honoured.

- The *third pillar* of the new Protocol concerns negative rules on extraterritorial and re-territorial government measures. This pillar should specify what sort of government regulation is prohibited. Its objective is to ensure that internet openness is protected and that there is greater clarity concerning the rights that other signatories have to transport data across borders. It follows the standard template of a trade agreement, where mechanisms for collaborative government-to-government behaviour are combined with rules describing what governments are not allowed to do. It gives economic significance to law enforcement collaboration and promotes its role. It also gives another reason for countries to subject themselves to stronger disciplines on law enforcement assistance. Under the current regime, some powerful countries sign agreements or treaties in order to get access to foreign assistance – while in effect reserving the right to unilaterally neglect requests made to them. One way to get them more interested in mutual assistance is to charge the system with an economic value – or, to put it differently, to raise the opportunity cost for uncooperative behaviour.

This structure prompts the question of which country should participate. Trade agreements and MLATs are often limited in reach – they only contain a few countries, while a multilateral treaty under the auspices of the UN system includes most countries in the world (and becomes subject to a lengthy process of compromises, if it's even feasible). Any effective legal assistance protocol is likely to be a plurilateral agreement between a smaller subset of countries that are willing to take on commitments equal to and beyond the Convention on Cybercrime and the next generation trade agreements where such commitments may come in. The high level of commitments would be a qualification process in itself: membership would require a 'due diligence' of the laws and institutions of a signatory.

The core political economy of a Multilateral Legal Assistance Protocol is that effective legal assistance precludes regulations with the intention or the effect of re-territorialising data. This is an important dimension of the proposed Protocol. One purpose of the Protocol is to invalidate current reasons for localisation rules. A protocol based on upward harmonisation – seeking a high rather than low common denominator – would by necessity be limited to the countries whose laws today reflect the principles and safeguards enshrined in the Convention on Cybercrime. Yet the Protocol should also be specific on its negative rules against localisation. It should serve as a platform for what individual members of the Protocol will do in its bilateral negotiations with non-member countries over mutual legal assistance and trade.

BIBLIOGRAPHY

LEGAL CASES

- Sarl Louis Ferarud v Viewfinder, 489 F 3d 474, New York, 2007
- Yahoo v LICRA, TGI de Paris, 2000
- World Trade Organization, US – Online Gambling (DS285)
- World Trade Organization, China – Publications and Audiovisual Products (DS363)

LEGAL TEXTS AND TREATIES

- Brazil, Marco Civil da Internet, PL 2126/2011
- Council of Europe, Convention on Cybercrime, CETS No. 185, 23/11/2001
- Council of the European Union, Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union
- European Commission, COM(2012)11, January 25th, 2012
- European Commission, E-Commerce Directive, 2000/12/EC
- European Commission, Directive on privacy and electronic communications, 2002/58/EC
- WIPO Copyright Treaty (WCT)
- WIPO Performance and Phonogram Treaty (WPPT)
- World Trade Organization, General Agreement on Trade in Services (GATS)
- World Trade Organization, E-Commerce Moratorium

LITERATURE

- Bauer, Erixon, Krol, Lee-Makiyama, The importance of getting data privacy right, US Chamber of Commerce, 2013
- Blackmer, W. Scott, Transborder data flows at risk, Information Law Group, accessed from: http://www.infolawgroup.com/2012/02/articles/cloud-computing-1/transborder-data-flows-at-risk/
- Lee-Makiyama, European leaders should leave data flows open, Euractiv, September 30th, 2013, accessed from: http://www.euractiv.com/infosociety/european-leaders-leave-data-flow-analysis-530785
- OECD Council Recommendation on Principles for Internet Policy Making, 2011
- Wu, Tim, Is Internet exceptionalism dead? TechFreedom, 2010
- United Nations Congress on Crime Prevention and Criminal Justice, Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime: Working paper prepared by the Secretariat, 22 January, 2010
- International Chamber of Commerce, ICC policy statement on Using Mutual Legal Assistance Treaties (MLATs) To Improve Cross-Border Lawful Intercept Procedures, No. 373/512m 12 September 2012,

LATEST PUBLICATIONS:

The Case for an EU-China investment agreement
ECIPE Bulletin No. 06/2013
By Michal Krol

Argentina, the Expropriation of Repsol YPF, and the Case for Improved Investment Protection Accords
ECIPE Policy Brief No. 08/2013
By Fredrik Erixon, Lisa Brandt

Who's Afraid of China's High-Tech Challenge?
ECIPE Policy Brief No. 07/2013
By Guy de Jonquières

Biofuels Reform in the European Union: Why New ILUC Rules will Reinforce the WTO Inconsistency of EU Biofuels Policy
ECIPE Occasional Paper No. 03/2013
By Fredrik Erixon

Solar Panels, Telecommunication Equipment – and the "Modernisation" of EU Trade Defence Policy
ECIPE Bulletin No. 05/2013
By Fredrik Erixon

China's Rise: Perceptions and Misperceptions
ECIPE Policy Brief No. 06/2013
By Krishnan Srinivasan

Serious China: The Rise of China and EU Implications
ECIPE Policy Brief No. 05/2013
By Frank Lavin

Can Europe overcome its conservatism? – Future of Europe from a Japanese perspective
ECIPE Bulletin No. 04/2013
By Takayuki Sumita

EU Policies on Online Entrepreneurship: Conversations with U.S. Venture Capitalists
ECIPE Occasional Paper No. 02/2013
By Fredrik Erixon

Price Tagging The Priceless: International reference pricing for medicines in theory and practice
ECIPE Policy Brief No. 04/2013
By Lisa Brandt

Money Mischief in the Eurozone: Reforming the European Monetary Union
ECIPE Occasional Paper No. 01/2013
By Fredrik Erixon

Mixing Apples and Oranges: The Limitations of Trade Policy in Mitigating Climate Change
ECIPE Bulletin No. 03/2013
By Lisa Brandt

One Year After the Foul Expropriation of YPF: Argentina's Road to Ruin
ECIPE Bulletin No. 02/2013
By Fredrik Erixon

On Camels and the Making of EU Biofuels Policy
ECIPE Bulletin No. 01/2013
By Fredrik Erixon

Openness in Public Procurement Markets: Time for a Reality Check
ECIPE Policy Brief No. 03/2013
By Patrick Messerlin

A fibre-rich diet for Europe: Is the EU's Next Generation Access strategy compromising on competition?
ECIPE Policy Brief No. 02/2013
By Lisa Brandt, Hosuk Lee-Makiyama

The European Centre for International Political Economy (ECIPE) is an independent and non-profit policy research think tank dedicated to trade policy and other international economic policy issues of importance to Europe. ECIPE is rooted in the classical tradition of free trade and an open world economic order. ECIPE's intention is to subject international economic policy, particularly in Europe, to rigorous scrutiny of costs and benefits, and to present conclusions in a concise, readily accessible form to the European public. We aim to foster a "culture of evaluation" – largely lacking in Europe – so that better public awareness and understanding of complex issues in concrete situations can lead to intelligent discussion and improved policies. That will be ECIPE's contribution to a thriving Europe in a world open to trade and cross-border exchange.

www.ecipe.org
Phone +32 (0)2 289 1350. Fax +32 (0)2 289 1359. info@ecipe. org. Rue Belliard 4-6, 1040 Brussels, Belgium