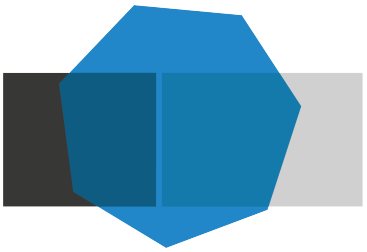


INTERNET
& JURISDICTION
POLICY NETWORK

DATA & JURISDICTION POLICY OPTIONS

CROSS-BORDER ACCESS TO USER DATA

November 2017

Input Document for Workstream I of the second Global Internet and Jurisdiction Conference

GLOBAL INTERNET AND JURISDICTION CONFERENCE 2018
FEBRUARY 26-28 • OTTAWA, CANADA
conference.internetjurisdiction.net

@IJurisdiction
www.internetjurisdiction.net

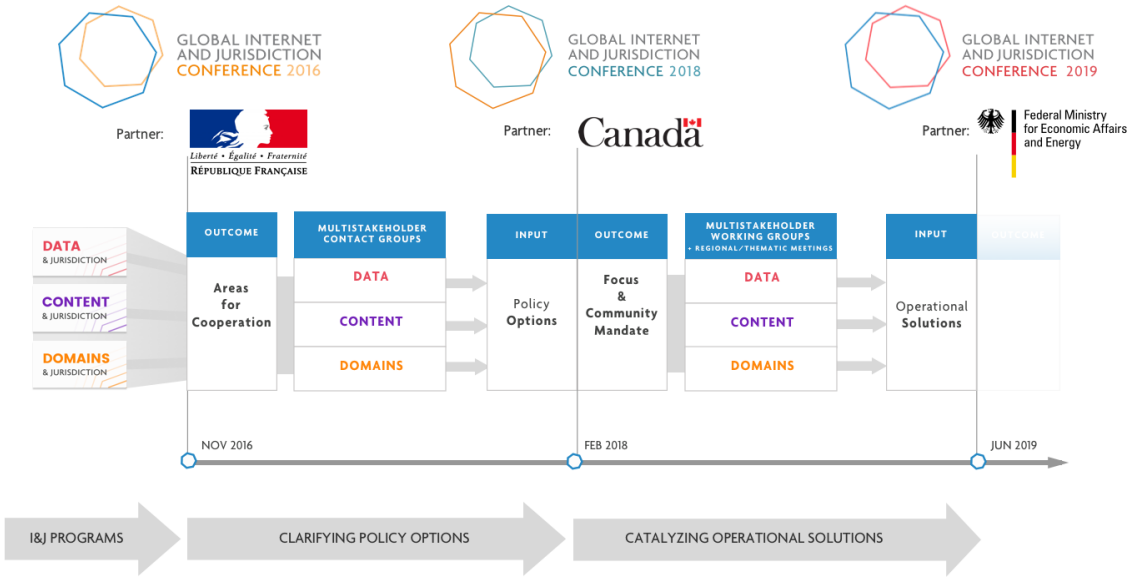
This Policy Options document prepared by the Secretariat of the Internet & Jurisdiction Policy Network presents the results of the work of the multistakeholder Data & Jurisdiction Contact Group. This Group was set up as a result of the first Global Internet and Jurisdiction Conference of the Policy Network, held in Paris on November 14-16, 2016, and which gathered 200 senior-level participants from 40 countries. The Group held seven virtual meetings in 2017 to explore the Areas of Cooperation identified in Paris (see Data & Jurisdiction Framing Paper[1]).

Reflecting preparatory work, this document will serve as input to structure discussions in Workstream I on Data & Jurisdiction on Day 2 of the second Global Internet and Jurisdiction Conference in Ottawa[2] on February 26-28, 2018. On this basis, stakeholders are expected to agree there on focus and community mandates to structure further work in the Internet & Jurisdiction Policy Network.

Feedback on this document can be submitted to the Secretariat until January 26, 2018 via gijc2018-data@internetjurisdiction.net. It will be shared with the Members of the Contact Group.

AN ONGOING PROCESS TOWARDS OPERATIONAL SOLUTIONS

The second Global Internet and Jurisdiction Conference of the Internet & Jurisdiction Policy Network is organized in partnership with the Government of Canada, and institutionally supported by OECD, UNESCO, Council of Europe, European Commission, and ICANN. It will be a milestone moment to identify concrete focus and priorities to develop policy standards and operational solutions to major jurisdictional challenges. This will define the methodology and roadmap in the lead-up to the third Global Internet and Jurisdiction Conference in June 2019, which will be organized in partnership with the Government of Germany.



ABOUT THE DATA & JURISDICTION CONTACT GROUP

The Contact Group was set up under the Data & Jurisdiction Program of the Internet & Jurisdiction Policy Network. Parallel Contact Groups have been established in the Content & Jurisdiction and Domains & Jurisdiction Programs, as well. The Group is composed of Members of different stakeholder constituencies, actively involved in addressing the jurisdictional challenges related to cross-border access to user data. This neutral space allowed participants to map their respective perspectives, compare approaches, foster policy coherence, and identify possible steps for coordinated actions.

---

[1] Secretariat of the Internet & Jurisdiction Policy Network (2017). Framing Paper of the Data & Jurisdiction Program https://www.internetjurisdiction.net/publications/paper/data-jurisdiction-program-paper

[2] https://conference.internetjurisdiction.net

Members of the Contact Group are:

- **Kevin Bankston**
  Director
  Open Technology Institute
- **Eduardo Bertoni**
  Director
  Data Protection Authority (DNPDP), Argentina
- **Jennifer Daskal**
  Associate Professor
  American University Washington College of Law
- **Lanah Kammourieh Donnelly**
  Public Policy Manager
  Google
- **Jane Horvath**
  Senior Director, Global Privacy Law and Policy
  Apple
- **Mark Lange**
  Director, EU Institutional Relations
  Microsoft
- **Greg Nojeim**
  Senior Counsel and Director, Freedom, Security And Technology Project
  Center for Democracy & Technology
- **Alexander Seger**
  Executive Secretary,
  Cybercrime Convention Committee
  Council of Europe
- **Dan Svantesson**
  Co-Director of The Centre For Commercial Law
  Bond University
- **Robert Young**
  Legal Counsel,
  Criminal, Security, and Diplomatic Division
  Global Affairs Canada
- **Cathrin Bauer-Bulst**
  E-Evidence Task Force
  DG Home, European Commission
- **Aaron Cooper**
  Counsel to The Assistant Attorney General, Criminal Division
  United States Department of Justice
- **Fernanda Domingos**
  Federal Prosecutor
  Federal Prosecutor's Office of the State of São Paulo, Brazil
- **Brendan Eiffe**
  Head, Central Authority for Mutual Legal Assistance
  Department of Justice and Equality, Ireland
- **Gail Kent**
  Global Public Policy Manager
  Facebook
- **Brad Marden**
  Assistant Director Digital Crime Investigative Support
  Interpol
- **Erik Planken**
  Senior Policy Advisor on Cybercrime
  Ministry of Security and Justice, The Netherlands
- **Christoph Steck**
  Director, Public Policy and Internet
  Telefonica
- **Peter Swire**
  Professor of Law and Ethics
  Georgia Tech University

ABOUT THE INTERNET & JURISDICTION POLICY NETWORK

The Internet & Jurisdiction Policy Network addresses the tension between the cross-border nature of the internet and national jurisdictions. Its Paris-based Secretariat facilitates a global multistakeholder process to enable transnational cooperation. Participants in the Policy Network work together to preserve the cross-border nature of the Internet, protect human rights, fight abuses, and enable the global digital economy. Since 2012, the Internet & Jurisdiction Policy Network has engaged more than 200 key entities from governments, Internet companies, technical operators, civil society, academia and international organizations around the world. Its Secretariat has convened, organized or contributed to more than 120 policy events in over 30 countries.

Data & Jurisdiction Policy Options

This document aims to provide, in a forward-looking approach, guiding elements to structure further discussion at the second Global Internet and Jurisdiction Conference in Ottawa on February 26-28, 2018, and beyond regarding cross-border access to digital evidence in the cloud, in order to reconcile high human rights standards and procedural efficiency in criminal investigations.

Criminal investigations increasingly require access to digital evidence stored by private companies from jurisdictions outside the requesting country. Yet, existing systems for such cross-border access to user data are under stress: Mutual Legal Assistance Treaties (MLATs) are slow and ill-adapted while limited procedural guarantees apply to direct requests to companies, which can even be forbidden by national blocking statutes such as the US Electronic Communications Privacy Act (ECPA). This can hamper legitimate investigations and the absence of agreed frameworks encourages mandatory data localization laws that are technically difficult to implement and have detrimental effects for the cloud economy, innovation and human rights.

Different efforts, referenced in the Framing Paper[3] of the Data & Jurisdiction Program of the Internet & Jurisdiction Policy Network produced after the first Global Internet and Jurisdiction Conference in Paris in 2016[4], are underway to find solutions. In particular, the US Department of Justice has proposed legislation that would enable the US government to make bilateral executive agreements with countries it would accredit (starting with the U.K.), allowing them to submit direct requests for content data to US companies. However, such a hub and spoke architecture - US-centered because of the dominance of American companies and the blocking statute of ECPA - will not easily scale into a general regime for access to evidence in the cloud. Yet, such scalability will likely be necessary as major global providers will increasingly be based in diverse countries. A more general framework would alleviate the need for a proliferation of bilateral agreements: a set of appropriate standards and procedures could be developed to be used as reference in successive agreements and in companies' Terms of Service[5].

This document explores possible components for such a voluntary framework and how to foster regime scalability. The focus is on cross-border access to *stored* data. Interception and encryption are not directly addressed and require separate discussions.

---

[3] See the I&J Data & Jurisdiction Framing Paper released after the first Global Internet and Jurisdiction Conference held in Paris in November 2016: https://www.internetjurisdiction.net/publications/paper/data-jurisdiction-program-paper

[4] See: https://conference2016.internetjurisdiction.net

[5] An analogy can be made here with the architecture (not the dispute resolution mechanism through arbitration) of the Uniform Dispute Resolution Procedure established by ICANN, where the UDRP policy is explicitly referenced in the accreditation agreements of registries and registrars and their contracts with registrants.

1. Framework Components

A common goal for actors could be to:

- Develop a framework with high substantive and procedural standards
- allowing relevant authorities from specific countries,
- in investigations regarding certain types of crimes with clear nexus with the requesting country,
- to directly submit structured and due process-respecting requests,
- to private companies in another country to obtain the voluntary disclosure
- of user data, irrespective of where such data is stored.

The above components[6] are detailed below in order to help structure future discussions.

Framework - Coordinated efforts among the different actors would entail: a modification of national legislations to remove potential blocking constraints; appropriate criteria regarding acceptable requests and beneficiary countries; implementation by the latter of corresponding national procedures; clarification of the conditions under which companies will handle such requests; and definition and implementation of transparency, redress and oversight mechanisms.

High standards - In spite of their limitations, MLATs with the US have clearly specified scopes and impose the high standard of "probable cause" and other US procedural guarantees. Any streamlined and more efficient regime should have criteria and procedures for both country accreditation and requests evaluation representing sufficiently high and robust protections.

Specific Countries - A bulk and unconditional removal of blocking provisions in ECPA would put on companies the entire responsibility to be arbitrators without clear protections. An accreditation mechanism for interested countries using a statutory set of requirements is necessary[7] but a very detailed and precise evaluation standard is difficult to set, given the diversity of national procedures.

Accreditation would therefore amount to an evaluation of human rights protections, including data protection, due process and judicial oversight, in the legal system of a country and specifically its national procedures for requesting stored user data. The current proposals envisage a series of “factors” for such decision but some actors advocate for more constraining “requirements”, inter alia to limit the risks of politically motivated evaluations.

Such accreditation should be for a limited duration with regular evaluation and review, under the responsibility of a government agency or agencies. The role of national legislatures in such accreditation and review procedures is important and should be clearly defined.

---

[6] These elements are not exhaustive and others may be identified in further discussions

[7] Although there are important differences, some draw an analogy with the mechanisms of visa waiver programs, which rely on national statutory frameworks setting criteria for other nations to qualify and a principle of reciprocity. The system can then grow through each nation meeting listed criteria, without the need for a treaty.

Relevant authorities - Certain levels of authority and prior procedure would be required for issuing requests. National points of contact would validate and channel them to similar points of contact in companies. A single registry or a distributed set of registries could record these authenticated channels, and be managed by existing or new dedicated structures.

Scope and types of crimes - To set an achievable bar, the focus should be, at least initially, on a subset of investigations. The general seriousness of the investigated crime (assessed through the level of penalty, for instance more than a certain number of years of prison) is an important factor, but may not be a sufficient nor exclusive one: some types of crimes with significant penalties need to remain out of scope, for example due to human rights considerations.

Various options can be envisaged to define the regime scope, including: an explicit and exhaustive list, a generic category with examples (serious crimes, including A, B, C) or exclusions (serious crimes, except A, B, C). Crimes out of scope would remain covered by the normal MLAT procedures.

Clear nexus - The discussed framework intends to address situations where the requesting country has a substantial connection to, and legitimate interest in, the data stored by a foreign provider. Multi-factor assessment of this nexus can include, when known: the nationality and habitual residence of the victim(s) and the suspect(s) and the location where the investigated crime was instigated or has its effect(s).

Some balance between the interests of the investigating state and other interests would also be required. In particular, specific provisions - maybe even exclusions - should be made for investigations targeting a national or resident of the country of incorporation of the service. Comity considerations also require further discussion regarding possible notification to third party countries, i.e. when a request from country A to a company in country B targets a national or resident of a third one C, in particular if an MLAT agreement exists between countries A and C. Other elements to be considered include the interest of the legal or natural persons involved, particularly privacy and the interest of the company holding the data not to be subject to conflicting claims from different countries forcing non-compliance with one law to abide by the other.

Structured requests - Defining what properly documented requests should contain would help interactions between actors and set a high procedural standard. A list of such elements includes: identification of sender and recipient, national legal basis and procedure followed (including existence of a court decision), type of investigation, specifics of the case, targeted person and account(s), data requested, and justification of necessity, proportionality and urgency (if any). Request submission formats could be jointly developed in that context.

Transmission of very detailed requests to private entities raises issues of confidentiality. Furthermore, the amount of necessary information is directly related to the degree of discretionary responsibility expected from or desired by the companies. An agreed list of elements could thus preferably constitute a standard for requests preparation and validation by local authorities (also see Q-SPOC discussion below), even if only some information is ultimately transmitted to companies.

An important part of such an individual request standard (as opposed to the standard for country accreditation) would be a sufficient equivalent to the "probable cause" rule in the US system. A formulation suggested in 2016 that could be discussed further was: "*a strong factual basis to believe that a crime has been, is being or will be committed and that the item sought is contraband or evidence of such a crime*".

Due process - Important elements in that regard include the following.

Independent authorization — An independent person or entity should decide whether there is sufficient justification for a demand for content data. Preferably, that decision maker would be a member of the judiciary.

Notification - User notification is a key component of due process offline as a condition for recourse. It should be transposed online and some companies already notify their users of government requests for data. A major challenge however is to avoid jeopardizing investigations: proper justification can establish ground for delayed notification, albeit within a reasonable timeframe. A formulation was explored according to which: "*Notice is required from governments and permitted from companies. It can be delayed under clearly defined conditions so that it does not compromise investigations*".

The intermediary may be the only actor able to contact the user and therefore the proper channel even for a notification by the requesting government. Requests for non-content data could be directed at the service provider but requests for content forwarded to the ultimate controller of the data, with appropriate mechanisms developed to ensure preservation of the data.

Another issue to address is how to prevent interferences or conflicts between different investigations, including via potential notification to LEAs regarding requests to providers in their country.

Capacity to object - When user notification can take place before disclosure, the conditions and procedures under which the targeted user can object to it have to be developed. This will prove in any case a challenging task in a cross-border environment.

Recourse and redress - Regardless of whether user notification is provided before or after disclosure, availability of recourse is essential. Like above, identifying the proper mechanisms will be challenging in transnational situations. Regarding redress, classic rules of criminal procedure would probably justify an inability to use inappropriately obtained evidence in related national procedures. In such case, major tasks will be to define the entity(ies) responsible for evaluating this inappropriateness and the criteria to do so, as well as ways to introduce such a remedy in national laws and jurisprudences.

Companies in another country - The rules regarding personal jurisdiction over internet companies incorporated in another territory are still imprecise and in flux. The criterion of "provision of service" is however gaining some traction[8]. It could lead to a distinction between production orders and mere production requests with different enforceability levels and presumption of compliance, in particular when a foreign operator has local offices in the requesting country. This document however is focused on the handling of production requests in a voluntary regime.

Voluntary disclosure - Companies do not want to be the sole arbiters of the appropriateness of requests, nor should they. Yet, absence of a blocking statute would only *allow* them to respond to a request from foreign countries participating in the regime, without clearly specifying when companies should accept it.

---

[8] The T-CY Committee in the Council of Europe has issued a guidance note on article 18 of the Cybercrime convention that clarifies this notion in the context of access to subscriber information. See: https://rm.coe.int/16806f943e

This means that they would have some discretion to refuse it. Should a company have doubts regarding whether a request meets the agreed standard in the regime, different paths could be available:

- Direct interaction with the requester's point of contact for additional information,
- Using the MLAT process as fallback mechanism,
- Soliciting advice, without penalty for delay, from the public authorities of its country of incorporation or, more innovatively, from some new multistakeholder advisory body.

Communication data - The main objective of such a regime would be to address the problem of *content* data, currently not accessible through direct cross-border requests to US companies. However, in the context of this discussion, some argue that strong criteria for voluntary disclosure by companies of *non-content data* (basic subscriber information, traffic data) to foreign law enforcement, currently absent from ECPA, should also be clearly defined.

Certain users - Specific provisions might be necessary concerning targeted users who are not known national or residents of the requesting country, such as:

- Nationals or residents of the country of incorporation of the company,
- Nationals or residents of a third country participating in the regime,
- Nationals or residents of a third country not participating in the regime, or
- Users whose nationality or residence is undetermined.

Data protection regimes also need to be taken into account as communication of content data can be considered treatment of personal information.

Irrespective of data location - Location of the physical carriers of the information to be accessed as a criteria for jurisdiction and proxy for control has a long legal history. However, the connection is harder to make in the age of cloud-based storage. There would be a strong benefit in moving away from this criteria and replacing it by the notion of control[9] of the data. A proper regime should establish the conditions of access to evidence in the cloud, irrespective of where it is physically stored.

Special attention needs to be paid to the chain of custody of the data: cloud operators often provide back-end capacity to other services that exercise the actual control over the data being sought. As custodian, the cloud provider should be tasked with channeling the requests to this ultimate recipient rather than be asked to communicate data that it does not directly control. This of course introduces additional complexities given the number of potential actors and jurisdictions involved.

2. Regime Scalability

Even if a regime starts with a few countries, it needs to be scalable to several others to deal with the long-term development of the cloud economy and reduce incentives for mandatory data localization. However, only in a very limited number of countries will the entire legal system meet the required high standard for their accreditation and the receivability of all their requests. To alleviate this problem, an additional step could be established by aspiring countries.

---

[9] This concept is distinct from the notion of data controller in privacy protection regimes.

Qualifying SPOCs - A central office could serve as Qualifying Single Point of Contact. Subject to review and with strict procedures, it could evaluate, qualify and certify that specific individual requests from that country meet the agreed standards. In particular, this Q-SPOC could ensure a step of independent judicial review, to meet the global standard when the national procedures do not require it. This Q-SPOC would not be tasked with second-guessing the national procedure followed, but rather with giving a stamp of approval by "checking that all the procedural requirements boxes have been ticked".

Independence - Such Qualifying SPOCs would be part of the country governance system, preferably directly connected to the judiciary. Independence would be strongly recommended, even if the designation of the entity or person were to be made by the government. Precedents do exist of such independent actors, connected to the judiciary, having the authority to make decisions on specific matters.

Oversight - Accreditation of a country would entail an evaluation of both its general legal system and the nature, functions and procedural rules of such a certifier. Regular review of such accreditation would alsoinclude review of the certifier. Creation of an independent review mechanism (for instance a multi-stakeholder advisory body) could be envisaged to contribute to this oversight function.

Embedding - The approach proposed by the US Department of Justice envisages an enabling legislation and a series of bilateral executive agreements. Embedding the above-discussed standards in the enabling legislation would provide predictability and confer a central role to Congress, with the potential drawback of rigidity. Embedding them in each respective agreement would provide more flexibility but also less control against a progressive negative evolution of protections as more countries are integrated in the regime. As an alternative, a self-standing common policy standard could be used as reference for legislations, agreements and companies Terms of Service.

As mentioned above, a hub and spoke architecture centered on the United States will not easily scale to provide a general regime for access to evidence in the cloud. On the basis of the above components, a critical mass of actors could initiate a common regime, with appropriate conditions for its ulterior expansion.

Annex

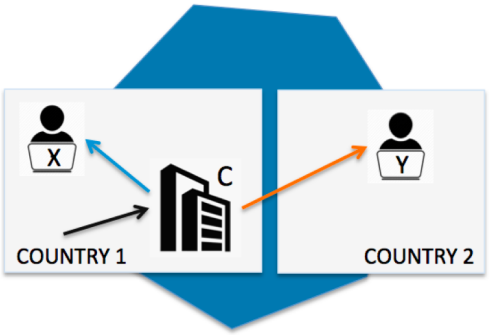
The following infographics aim to describe the different situations that can be encountered in the context of requests for disclosure of user data. They might help evaluate how any envisaged cloud evidence regime would function in each case. The elements described above relate to situations 3 to 6. (Note: in the drawings below, countries 1 and 2 are supposed part of the regime).

SITUATION 1

Country 1 LEA requests from company C in **country 1** data about **user X** who is a national or resident in **country 1**

SITUATION 2

Country 1 LEA requests from company C in **country 1** data about **user Y** who is a national or resident in **country 2**

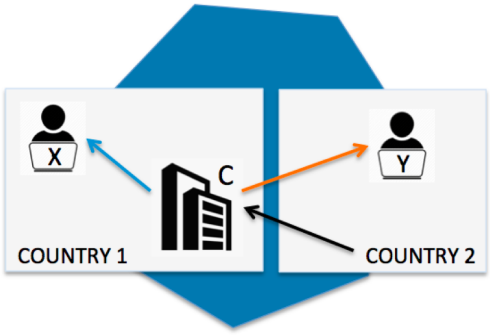


SITUATION 3

Country 2 LEA requests from company C in **country 1** data about **user X** who is a national or resident in **country 1**

SITUATION 4

Country 2 LEA requests from company C in **country 1** data about **user Y** who is a national or resident in **country 2**



SITUATION 5

Country 2 LEA requests from company C in **country 1** data about **user Z** who is a national or resident in **country 3, part of the regime**

SITUATION 6

Country 2 LEA requests from company C in **country 1** data about **user T** who is a national or resident in **country 4, not part of the regime**