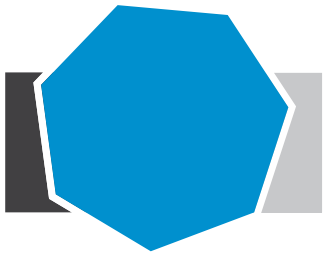


INTERNET & JURISDICTION POLICY NETWORK

DATA & JURISDICTION PROGRAM

OPERATIONAL APPROACHES
NORMS, CRITERIA, MECHANISMS

APRIL 2019
www.internetjurisdiction.net

FOREWORD

When the Internet & Jurisdiction Policy Network was founded in 2012, the importance of addressing jurisdictional issues online was hardly recognized by most stakeholders. The dominant view was simply that the anticipated mass increase in internet penetration would allow people around the world to better connect and share their ideas, contribute to greater freedom and create new economic opportunities. To a large extent, many aspects of this vision have materialized in the past seven years and we now take for granted the many benefits this unprecedented collective creation of mankind has brought.

In spite of that - or maybe because of it - attention in recent years has significantly shifted: hardly a day passes without major newspapers headlines about abuses online and the difficulty to address them, given the transnational nature of the network. We may rationally recognize that such abuses remain limited in proportion of the overall online activity, but the tremendous volume of the latter legitimately make the former an increasing concern for all actors. Addressing harmful content, criminal activities and other regulatory challenges in a rights-respecting and economically sustainable manner has emerged as a crucial question for the digital 21st century.

It may have been naive to think that the dark side of human nature would not express itself also in the digital space, but it behooves all of us now to avoid letting the pendulum swing too far in the other direction. We need to find collective solutions that not only protect the precious acquis of a global network but enable our digital society to develop further in a balanced manner. This can only be achieved through cooperation similar to that which enabled the emergence of the internet itself. Unfortunately, the existing international system of separate territorial sovereignties often represents an obstacle to such cooperation.

In the absence of clear international arrangements, after a long period of inaction, the last few years have witnessed a number of separate proposals and regulations to address abuses online. However well intentioned some of them may be, unilateral decisions adopted in an uncoordinated manner under the pressure of urgency may have detrimental unintended consequences. Yet, the very proliferation of initiatives demonstrates a shared concern to address these issues. This convergence in the willingness to act must be accompanied by increased communication, coordination and cooperation between actors. It is more than ever crucial to reiterate our firm belief in the necessity to tackle common problems in a collective manner.

Given the evolution in actors' mentalities, discourse and actions that we have witnessed in the past seven years, in particular in the context of the Internet & Jurisdiction Policy Network, we should be optimistic that we can develop common frameworks benefiting all stakeholders. By working intensely and in a constructive spirit in relentless pursuit of scalable, interoperable and resilient solutions, we can together address the most pressing issues of the digital society. The following *Operational Approaches* document represents an encouraging step in this direction, concretely illustrating what can be produced when actors commit to working together in pursuit of the common public interest.

Bertrand de La Chapelle

Executive Director

Secretariat of the Internet & Jurisdiction Policy Network

TOWARDS LEGAL INTEROPERABILITY

The Internet increasingly underpins political, economic and social interactions. However, as Internet penetration grows, so do cross-border legal problems. The transnational nature of the network challenges the territorial foundation of national legal systems. The number of internet users more than doubled in the last decade, and more than half the world's population is now online. How to jointly address pressing legal challenges at the intersection of the global digital economy, human rights and security has become one of the greatest challenges of the 21st century that will define the future of the cross-border internet and the digital society.

Since 2012, stakeholders from around the world work together in the Internet & Jurisdiction Policy Network to address the tension between the cross-border nature of the Internet and national jurisdictions. Its Secretariat enables multistakeholder cooperation and facilitates a global policy process engaging over 200 key entities from more than 40 countries and all stakeholder groups: governments, the world's largest internet companies, technical operators, civil society groups, academia and international organizations.

Stakeholders in the Internet & Jurisdiction Policy Network work together in currently three thematic Programs (Data & Jurisdiction, Content & Jurisdiction and Domains & Jurisdiction) to jointly develop policy standards and operational solutions through regular virtual and physical meetings, including regional sessions and Global Conferences. The Secretariat also maintains the I&J Retrospect Database tracking global trends, and launches in 2019 the world's first Internet & Jurisdiction Global Status Report.

The regular Global Conferences of the Internet & Jurisdiction Policy Network are institutionally supported by six international organizations: Council of Europe, European Commission, ICANN, OECD, United Nations ECLAC, and UNESCO. They were organized in the past in partnership with France (2016) and Canada (2018). The work of stakeholders in the Internet & Jurisdiction Policy Network has been presented to and recognized by key international processes, including the United Nations Internet Governance Forum, G7, G20 or the Paris Peace Forum, and covered in media outlets such as The Economist, New York Times, Washington Post, Financial Times, Politico or Fortune. The work of the Policy Network is financially supported by a unique coalition of over 20 governments, companies and organizations.

FROM ISSUES FRAMING TO AREAS OF COOPERATION

After four years of international consultations and meetings in the Internet & Jurisdiction Policy Network, stakeholders gathered for the first time on a global level in Paris on November 14-16, 2016 to address the future of jurisdiction on the cross-border Internet. On this occasion, over 200 senior representatives from all stakeholder groups stressed the urgency of finding mechanisms for communication, coordination and cooperation in order to establish legal interoperability and ensure due process across borders. At this 1st Global Conference, they recognized that no actor or stakeholder group can solve these new challenges on their own: collective action was needed to prevent the escalation of a legal arms race and the proliferation of legal uncertainty. On the basis of *Framing Papers*[1] for each of the three thematic I&J Programs, they accordingly identified key *Areas for Cooperation*[2] to proceed together.

FROM POLICY OPTIONS TO THE OTTAWA ROADMAP

These *Areas for Cooperation* served as mandate for the three thematic Programs Contact Groups formed as a result of the 1st Global Conference. Composed of Members from a diverse range of entities

[1] https://www.internetjurisdiction.net/news/framing-papers-released-for-data-content-and-domains

[2] https://www.internetjurisdiction.net/uploads/pdfs/GIJC-Secretariat-Summary.pdf

and experts most engaged in the issues, they were tasked to propose what can realistically and pragmatically be achieved within each of the I&J Programs. Members, with the support of the Secretariat, mapped their respective perspectives, compared approaches, fostered policy coherence, and identified possible steps for coordinated actions. The results of these focused discussions were synthesized in *Policy Options* documents[3] released for stakeholder consultations in November 2017.

They served as official input to structure discussions at the 2nd Global Conference of the Internet & Jurisdiction Policy Network in Ottawa on February 26-28, 2018. Over 200 stakeholders from more than 40 countries decided there on concrete focus and priorities, agreeing for the first time on Common Objectives and Structuring Questions for each of the three Programs of the Policy Network. These Work Plans were consolidated in the *Ottawa Roadmap*[4].

OPERATIONAL APPROACHES

Building on the methodology of the work in the I&J Programs between the 1st and 2nd Global Conferences, over 120 Members from all continents and stakeholder groups officially begun their work in August 2018 in new Contact Groups to implement the Work Plans of the *Ottawa Roadmap*. Three neutral Coordinators were appointed to facilitate discussions. They were respectively:

- DATA & Jurisdiction: Robert Young, Legal Counsel, Global Affairs Canada.
- CONTENT & Jurisdiction: Wolfgang Schulz, Director, Humboldt Institute for Internet and Society.
- DOMAINS & Jurisdiction: Maarten Botterman, Director, GNKS Consult.

The Members of the three Programs' Contact Groups were committed to working together and develop operational policy approaches in preparation for the 3rd Global Conference of the Internet & Jurisdiction Policy Network. The mandate for the three Programs' Contact Groups was defined on the basis of the Structuring Questions of the *Ottawa Roadmap*'s Work Plans. Topic-specific Working Groups were established in each Program to conduct focused work and allow for more intense interactions on specific issues.

The *Operational Approaches* documents present the result of this process. They are a best effort by the Members of each Program's Contact Group to address the important cross-border issues pertaining to access to electronic evidence, content restrictions and moderation online, and requests for domain suspensions, in a manner consistent with due process and the protection of human rights.

THE 3rd GLOBAL CONFERENCE AND BEYOND

The 3rd Global Conference of the Internet & Jurisdiction Policy Network will be held on June 3-5, 2019, in Berlin, Germany. When they convene in Berlin stakeholders will discuss, on the basis of the *Operational Approaches*, how to advance the development of concrete policy standards and operational solutions. The *Berlin Roadmap* that will come out of this 3rd Global Conference will guide the next phase of work of stakeholders in the Programs of the Internet & Jurisdiction Policy Network, in particular:

- How proposals in the *Operational Approaches* documents (Norms, Criteria and Mechanisms) can be used to enhance legal interoperability,
- How to structure further work on issues already identified that require or warrant more in-depth discussions;
- How to address new issues identified at the 3rd Global Conference in a solutions-oriented manner.

[3] https://www.internetjurisdiction.net/news/policy-options-documents-released-for-the-2nd-global-internet-and-jurisdiction-conference

[4] https://www.internetjurisdiction.net/news/outcomes-of-the-2nd-global-conference-of-the-internet-jurisdiction-policy-network

CONTEXT

CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE - THE CHALLENGE

Access to electronic evidence has become central to law enforcement investigations regarding not only online crime but also illegal activities in the physical space. This increasingly requires access to electronic evidence stored[1] in the cloud by private companies in jurisdictions outside the requesting country.

According to a recent EU report[2] based on data from Member States and providers' Transparency Reports, electronic evidence in any form is relevant in around 85% of total criminal investigations. In almost two thirds (65%) of the investigations where electronic evidence is relevant, a request to service providers based in another jurisdiction is needed. As a result, 55% of total investigations require cross-border access to electronic evidence. This trend is expected to further accelerate.

In that context, existing mechanisms for cross-border user data requests are under stress:

- The system of Mutual Legal Assistance Treaties (MLATs) was initially designed to handle relatively rare cases, and is generally regarded as slow, complex and in need of reform. Even if improved, it is in any case ill-adapted to the fact that the very large majority of requests (94% for the EU) relate to investigations where the crime, the victim(s), and the perpetrator(s) are in the very country making the request.
- A large volume of the requests concern major providers based in the United States, but the existing framework of the 1986 Electronic Communications Privacy Act (ECPA) only allows voluntary communication by US companies of non-content data. This is the reason why most direct requests currently cover basic subscriber information and traffic data.

This situation creates significant legal uncertainty and the international legal architecture actually can prevent the cooperation necessary to address crime. Uncoordinated actions to address this challenge can have unintended consequences including increased conflicts of laws. Innovative thinking is required to develop, in addition to existing frameworks, cross-border cooperation mechanisms that fully protect citizen's rights and privacy, taking into account the established legal landscapes and investigatory procedures, and the differences in the size, nature and capacity of stakeholders.

Within each country, law enforcement investigations and access to electronic evidence are regulated according to strict national procedures, but with significant local differences. A common challenge for all actors is therefore to develop mechanisms allowing cross-border requests to providers for access to electronic evidence that are based on high standards of due process and protection of human rights.

The lack of clear mechanisms for cross-border access to electronic evidence incentivizes the introduction of mandatory data localization requirements. Beyond significant technical feasibility issues, the generalization of this approach would lead to major barriers for smaller economic actors, and endanger the cross-border nature of the internet.

More importantly, a significant evolution should be highlighted regarding the location of data. While location is a critical factor for physical evidence, the situation is markedly different for electronic evidence. Not only is it likely to be stored outside of the investigating country's territory, but the increasing use of cloud services makes the actual location more uncertain: it is determined for technical

[1] *This document covers access to stored data, not real-time interception. It also does not address the potential consequences of the growing use of encryption.*

[2] *See European Commission, "Commission Staff Working Document", p. 14-15, available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2018:0118:FIN:EN:PDF*

reasons rather than legal ones and the data can be split and distributed in several locations. It is thus being gradually recognized that lesser weight - if at all - should be ascribed to the storage location of the data sought. Any regime for cross-border requests to electronic evidence should ideally function irrespective of where the data is located.

EXISTING INITIATIVES

Actors within the ecosystem, and in the Data & Jurisdiction Program of the Internet & Jurisdiction Policy Network have expressed their interest in exploring how regimes that allow public authorities to issue requests for electronic evidence directly to service providers could function. In 2016, an objective was set to identify policy standards respecting privacy and due process, and defining the conditions under which authorized law enforcement authorities can request from foreign companies access to stored user data necessary for lawful criminal investigations.

The Data & Jurisdiction Program sought to address the following questions:

- How can transnational data flows and the protection of privacy be reconciled with lawful access requirements to address crime?
- What are the necessary safeguards and procedures to establish viable and scalable frameworks addressing the above question?

Recent specific initiatives explore different approaches to this issue, in particular:

- **The US CLOUD Act** was signed into law in March 2018. It contains two parts: it first establishes that US warrants served to US providers can apply to electronic evidence that they control, irrespective of its location; it also envisages that the blocking statute of ECPA would be lifted to allow providers to transfer data (including content data) to public authorities from foreign countries that have entered into an executive agreement with the United States.
- **The EU E-evidence Regulation Proposal** introduced by the EU Commission in April 2018, was revised by the European Council in November 2018 and is currently under review by the European Parliament. It envisages Production Orders allowing competent authorities from Member States to compel the transmission of electronic evidence (content and non-content) directly from operators that "provide services" to users in the EU. These providers would separately be required to designate a legal representative in the EU for that purpose.
- **An Additional Protocol to the Budapest Convention on Cybercrime** is currently being developed by the Cybercrime Convention Committee of the Council of Europe, to enable more efficient access to electronic evidence.

These proposals introduce or envisage different rules, safeguards and procedures to enable law enforcement authorities to issue cross-border requests or orders to service providers for access to electronic evidence.

A GENERAL FRAMEWORK

The work of the dedicated Contact Group of the Internet & Jurisdiction Policy Network, as presented in this *Operational Approaches* document, aims to contribute to this discussion by providing a general framework regarding the key components that regimes for cross-border requests should address, their potential scalability and how to foster interoperability between different such initiatives.

The Internet & Jurisdiction Secretariat

TABLE OF CONTENTS

COORDINATOR'S MESSAGE

It has been an honour to serve as the Coordinator of the Data & Jurisdiction Program's Contact Group. I can admit now that I accepted the role last year with some hesitation, for two reasons. First, because of the formidable, even daunting, expertise of the proposed Contact Group Members from around the world, which far exceeds my own. The second was the challenging nature of the issues to be addressed. I knew these are complex, and that reconciling diverse interests and perspectives to produce any useful results was far from guaranteed. Hence my hesitation.

Happily, my fears were unfounded on both fronts. The Contact Group Members shared their expertise generously, with patience, modesty and mutual respect, over countless hours of videoconference meetings of the Contact Group itself and its different Working Groups, not to mention the time spent in preparation and follow-up.

The Contact Group was diverse and truly global – it was a challenge for our hard-working Secretariat to schedule our meetings, with Members joining from multiple time zones across Europe, North America, Australia, Asia, Africa and South America. Beyond this geographical diversity, the Contact Group Members brought perspectives from all the stakeholder sectors that give the Internet & Jurisdiction Policy Network its legitimacy and strength – governments, the world's largest internet companies, technical operators, civil society groups, academia and international organizations.

I take this opportunity to express my sincere gratitude to the Contact Group Members for their engagement, their time and their consistently constructive approach. Special thanks are also due to the Facilitators who dedicated significant efforts to find formulations reflecting consensual positions within the Contact Group. It is the Members' expertise, global reach and diversity of perspectives, and their sustained commitment, that made possible the concrete outcomes of our work, reflected in this *Operational Approaches* document. Let me also express my gratitude to the Secretariat team in Paris without who the work would not be possible.

I truly believe that these outcomes will be of high practical value for many stakeholders grappling with the issues addressed by the Data & Jurisdiction Program, and that this will also provide a sound foundation for future discussions. I look forward to those exchanges, not only at the upcoming Global Conference in Berlin, but also in the follow-up work in the months and years to come.

Robert Young

Coordinator

Data & Jurisdiction Program's Contact Group

MEMBERS OF THE DATA & JURISDICTION PROGRAM'S CONTACT GROUP

The Secretariat appointed a neutral Coordinator to facilitate the work of the Contact Group:

- **ROBERT YOUNG**, Legal Counsel, Canada, Department of Global Affairs

The discussions in Working Groups, which helped conduct focused work on specific topics, were moderated by neutral Facilitators:

- **SHARON BRADFORD FRANKLIN**, Director, Surveillance and Cybersecurity Policy, New America Foundation's Open Technology Institute
- **DEBRAE KENNEDY-MAYO**, Research Faculty Member, Georgia Institute of Technology, Scheller College of Business

MEMBERS OF THE CONTACT GROUP

SUNIL ABRAHAM	Executive Director, Centre for Internet and Society
WAISWA ABUDU SALLAM	Head Legal Affairs, Uganda, Communications Commission
KAREN AUDCENT	Senior Counsel and Team Leader, Canada, Ministry of Justice
KERRY-ANN BARRETT	Cyber Security Policy Specialist, Organization of American States
CATHRIN BAUER-BULST	Deputy Head of Unit, Fight Against Cybercrime, European Commission, DG HOME
EDUARDO BERTONI	Director, Argentina, National Access to Public Information Agency
JOSEPH CANNATACI	Special Rapporteur on the Right to Privacy, United Nations
JENNIFER DASKAL	Associate Professor, American University Washington College of Law
FERNANDA DOMINGOS	Federal Prosecutor, Brazil, Federal Prosecution Service
BRENDAN EIFFE	Head, Irish Central Authority for Mutual Legal Assistance, Ireland, Department of Justice and Equality
THOMAS FITSCHEN	Director, Cyber Foreign Policy and Cyber Security, Germany, Federal Foreign Office
SHARON BRADFORD FRANKLIN	Director, Surveillance and Cybersecurity Policy, New America Foundation's Open Technology Institute
ERIC FREYSSINET	Chief Digital Strategy Officer, France, Gendarmerie Nationale
HARTMUT GLASER	Executive Secretary, Brazilian Internet Steering Committee (CGI.br)
NICOLE GREGORY	Head, Data and Online Harms Policy, United Kingdom, Foreign and Commonwealth Office
JANE HORVATH	Senior Director, Global Privacy, Apple
GAIL KENT	Global Public Lead on Law Enforcement and Surveillance, Facebook
MAY-ANN LIM	Executive Director, Asia Cloud Computing Organization
DREW MITNICK	Policy Counsel, Access Now
VIVEK NARAYANADAS	Data Protection Officer and Associate General Counsel, Shopify
GREG NOJEIM	Senior Counsel and Director, Freedom, Security and Technology Project, Center for Democracy & Technology

BARRACK OTIENO	General Manager, African Top-Level Domains Organization (AfTLD)
MARC PORRET	Senior Legal Officer, United Nations Counter-Terrorism Committee Executive Directorate (UNCTED)
KATITZA RODRIGUEZ	International Rights Director, Electronic Frontier Foundation (EFF)
ALBERTO RODRIGUEZ ALVAREZ	Advisor to the National Digital Strategy, Mexico, Office of the President
ALEXANDER SEGER	Executive Secretary, Cybercrime and Convention Committee and Head of Cybercrime Division, Council of Europe
ACADIA SENESE	Senior Counsel, Google
BERNARD SHEN	Assistant General Counsel, Microsoft
CHRISTOPH STECK	Director, Public Policy and Internet, Telefonica
DAN SUTER	Director, iJust
DAN SVANTESSON	Co-Director, Bond University, Centre for Commercial Law
PETER SWIRE	Professor, Georgia Institute of Technology, Scheller College of Business
CHRIS WILSON	Senior Manager, Public Policy (Internet Governance), Amazon Web Services
HERBERT GUSTAV YANKSON	Director of Cybercrime, Unit of the Criminal Investigations Department (CID), Ghana, Police Service
MOCTAR YEDALY	Head, Department of Information Society, African Union Commission
ROBERT YOUNG	Legal Counsel, Canada, Department of Global Affairs

In addition to the Members of the Contact Group, the Secretariat wishes to thank the following actors for their engagement in discussions held in the Contact Group and its Working Groups.

MELISSA BLAGITZ	Federal Prosecutor, Brazil, Federal Prosecution Service
DIEGO CANABARRO	Expert Advisor to the Board, Brazilian Internet Steering Committee (CGI.br)
ANDREA FABRA	Manager, Public Policy and Internet, Telefonica
CAMILLE FISCHER	Stanton Fellow, Electronic Frontier Foundation (EFF)
SEBASTIAN KAY	Head, EU and International Data, United Kingdom, Foreign and Commonwealth Office
DEBRAE KENNEDY-MAYO	Research Faculty Member, Georgia Institute of Technology, Scheller College of Business
EMMANUELLE LEGRAND	Legal and Policy Officer, European Commission, DG JUST
TOMA MILIESKAITE	Legal Officer, European Commission, DG JUST
HAN SOAL PARK	Associate Legal Officer, United Nations Counter-Terrorism Committee Executive Directorate (UNCTED)
KIMBERLY PEARCE	Counsel, Canada, Department of Justice
PALOMA VILLA MATEOS	Manager, Public Policy and Internet, Telefonica

SYNTHESIS OF THE OPERATIONAL APPROACHES

The following *Operational Approaches* document is the result of a best effort by the Members of the Data & Jurisdiction Program's Contact Group to address the important issues identified in the *Ottawa Roadmap* of the 2nd Global Conference of the Internet & Jurisdiction Policy Network on February 26-28, 2018. The Work Plan that was refined there identified 15 important Structuring Questions to further guide interactions within the Data & Jurisdiction Program. These *Operational Approaches* are a joint contribution by some of the most engaged experts in this field to advance the ongoing debate on the complex issues of cross-border access to electronic evidence. **They should however not be understood as the result of a formal negotiation validated by these Members' organizations.**

On this basis, the Program's Contact Group, with the help of the Secretariat, produced the attached set of proposed Operational Norms, Criteria and Mechanism that contain provisions that it recommends should be included in any framework (including applicable domestic laws and international agreements) for direct cross-border requests/orders by law enforcement to providers for electronic evidence. Some of the recommended provisions contain mandatory requirements (e.g., elements that must be met under the recommended approach), and some provisions are recommendations that may require further refinement or adaptation to meet the needs of particular countries.

Taking into account the limited time available to address these complex issues, the work of the Members of the Program's Contact Group was distributed among four thematic Working Groups, to propose, draft and refine elements that are documented according to the three-part structure presented on page 16.

These *Operational Approaches* will feed into the 3rd Global Conference of the Internet & Jurisdiction Policy Network on June 3-5, 2019 in Berlin, which is organized in partnership with the Government of the Federal Republic of Germany, and institutionally supported by the Council of Europe, European Commission, ICANN, OECD, United Nations ECLAC, and UNESCO.

STRUCTURE OF THE OPERATIONAL APPROACHES

The *Operational Approaches* document is organized according to the following three-part structure.

OPERATIONAL NORMS

This section identifies a set of norms that can help organize actors' own behavior and their mutual interactions. They focus on the operational level within the context of existing high-level principles.

The Data & Jurisdiction Operational Norms identify elements pertaining to any regime enabling cross-border access to electronic evidence, and to individual requests/orders.

OPERATIONAL CRITERIA

This section contains lists of elements or criteria that can be used by all categories of decision-makers when developing, evaluating, and implementing solutions. The purpose is for all actors to be able to discuss ideas, evaluate initiatives and debate proposals using common frames of reference and structuring questions.

The Data & Jurisdiction Operational Criteria address three important themes of the debate on access to electronic evidence: **(I) Regime standards** regarding scope (types of crime and data covered) , particular standards applicable to different types of actors (authorities, providers and users) and transparency/accountability mechanisms; **(II) Scalability**, taking into account the diversity of providers and of public authorities, and exploring models for geographic scalability; and **(III) Requests / orders standards** exploring the question of transmission of individual requests/orders, their necessary components and formats, and establishment of nexus by public authorities.

OPERATIONAL MECHANISM

This third section presents a proposal for which operationalization efforts can be initiated in the period following the 3rd Global Conference of the Internet & Jurisdiction Policy Network, in Berlin.

The concept note details the idea of interoperability tags for components of requests / orders, to allow transfer and handling of cross-border requests for electronic evidence in a manner that is efficient and respectful of high substantive and procedural guarantees.

OPERATIONAL NORMS

A general approach regarding cross-border access to electronic evidence can be based upon the following elements.

REGIME[1]

Any regime enabling cross-border requests/orders to providers for electronic evidence should duly address:

Due Process, so that:

- Commonly agreed high standards and procedural guarantees define the conditions under which public authorities can issue valid requests/orders and providers respond to them;
- Clear requirements and procedures for notification and avenues for recourse are available to providers and users;
- Relevant rules and procedures are transparently available and accessible to the public.

Scalability, so that the regime is able to:

- Manage a fast-growing number of requests/orders and flexibly adapt as necessary;
- Be resilient in a context of rapid technological evolutions;
- Accommodate relevant public authorities at various levels and providers with diverse roles, sizes and capacities;
- Progressively engage a growing number of diverse countries or be replicable in a sustainable manner, under strict fundamental requirements;
- Interoperate with other frameworks with similar purposes and same level of standards.

REQUESTS / ORDERS

Individual cross-border requests/orders for access to electronic evidence should enable verification of:

Completeness, including that:

- Verifiable authenticating information enables the receiver to confirm the country and entity making the request;
- Sufficiently detailed supporting information is provided, according to clear and agreed components of request formats, to enable the assessment of compliance with applicable domestic laws, and international law and the regime under which the request/order is issued.

Respect of relevant standards, in that the request/order:

- Is issued and written in full accordance with the provisions of the relevant national laws and of the regime under which it is submitted;
- Provides an independent certification that the agreed standard and minimal requirements for this specific type of request/order are met.

Nexus, through the establishment by the issuing country of:

- Its substantial connection to the crime;
- Its legitimate interest in obtaining the specific data sought;
- Its consideration of the potential interests of other actors.

Communication, coordination and cooperation between several countries may be necessary to guarantee respect of rights, ensure optimal efficiency, distribute responsibilities and avoid jeopardizing existing procedures.

---

[1] *A classical definition of an international regime is: "Implicit or explicit principles, norms, rules and decision-making procedures around which actors' expectations converge in a given area of international relations" - Krasner, Stephen D. 1983 in International Regimes, Cornell University Press. See also the definition of internet governance in the WSIS Tunis Agenda.*

OPERATIONAL CRITERIA

The following criteria represent the best efforts by the Members of the Data & Jurisdiction Program's Contact Group and its Working Groups, as compiled by the I&J Secretariat, in identifying concise lists of elements or criteria that can be used by all categories of decision-makers when developing, evaluating, and implementing solutions. The purpose is for all actors to be able to discuss ideas, evaluate initiatives and debate proposals using common frames of reference and structuring questions.

The following documents should be understood as basis for future reference and work in the Internet & Jurisdiction Policy Network, following its 3rd Global Conference. Below is the list of Operational Criteria for the Data & Jurisdiction Program:

PART I - REGIME STANDARDS

- CRITERIA A - Regime Scope
- CRITERIA B - Public Authorities
- CRITERIA C - Providers
- CRITERIA D - Users
- CRITERIA E - Transparency / Accountability

PART II - SCALABILITY

- CRITERIA F - Diversity of Public Authorities
- CRITERIA G - Diversity of Providers
- CRITERIA H - Geographic Scalability

PART III - REQUESTS / ORDERS STANDARDS

- CRITERIA I - Transmission
- CRITERIA J - Request Formats
- CRITERIA K - Nexus

PART I - REGIME STANDARDS

CRITERIA A - REGIME SCOPE

1. **Covered data:**
   Content and other private and protected information as defined by applicable law that is held by providers.
2. **Type of crime(s) covered:**
   Data requests/orders may be issued for the purpose of obtaining information likely to assist in the detection, investigation, or prosecution of crimes
   a. That are serious crimes[1]; and
   b. Where the detection, investigation and/or prosecution does not infringe on international human rights[2].

[1] There was no consensus on whether to add in "that are punishable in the requesting country by a sentence of at least 3 years" as a definition of serious crimes. This criteria leaves the term "serious crimes" undefined which would permit more variation among countries.

[2] The Group did not reach consensus on requiring dual criminality, but seeks safeguards against data requests/orders for prosecutions that would infringe international human rights law.

CRITERIA B - PUBLIC AUTHORITIES

1. **Degree of judicial/independent validation on a request-by-request basis (and emergency situations):**
   For each request/order for content or other private and protected information, the applicable domestic laws and/or international agreements should require mandatory prior review and approval by a court, judge, magistrate or other independent authority that is prescribed by law.
   Jurisdictions may choose to allow the following exceptions to the requirement for prior review and approval:
   a. for emergency situations involving imminent danger of death or serious physical injury to a person[1] in which case independent review and approval by a court, judge, magistrate or other independent authority that is prescribed by law is required to enable the requesting country to use the data after the emergency situation has ended; and
   b. for requests for preservation of the specific data sought, in which case the applicable domestic laws and/or international agreements requires independent authorization by a court, judge, magistrate or other independent authority that is prescribed by law before it could access and use the data.
   Countries should provide their independent authorities with sufficient resources to enable them to comply with the rules and standards of the regime.

[1] Some Members of the Group would like to add here "or imminent threat to critical infrastructure," but other members strongly oppose this addition. We note that this is an area where there is variation in approaches among different countries that may need to be resolved as international agreements are finalized.

2. **Standard of proof:**
   The standard for the review and approval (as specified in point 1 above) of data requests/orders should:
   a. mandate a strong legal and factual basis showing that the information sought is evidence of a crime that is under investigation and that is within the jurisdiction of the requesting country.
   b. be rigorous, providing protection for international human rights, including adequate protection for personal privacy according to international human rights.
3. **Necessity and proportionality:**
   Countries should mandate that requests/orders meet the standards of necessity and proportionality under international human rights law.

CRITERIA C - PROVIDERS

1. **Clarification of requests/orders:**
   The regime should establish a procedure that protects the rights of providers to seek clarification from requesting countries about data requests/orders.
2. **Challenges of requests/orders by provider:**
   a. The regime should establish a clear procedure for an independent authority to hear and adjudicate providers' challenges to data requests/orders.
   b. The regime should establish procedural and substantive rights for providers to challenge any data request/order[1] on the ground[2] that:
      i. the data request/order is overbroad, abusive, violates the terms of an international agreement or is otherwise unlawful;
      ii. the data request/order has been made for the purpose of prosecuting or punishing a person on account of that person's race, religion, nationality, ethnic origin, political opinion, gender or sexual orientation, and/or
      iii. compliance with the request/order would cause injury to that person for any of the reasons above, or would violate the international human rights of a person or the rights of a person under applicable laws;
   c. Providers should be able to request that the countries where their headquarters are located file objections to requests/orders when the provider believes the request/order has been made for the purpose of prosecuting or punishing a person on account of that person's race, religion, nationality, ethnic origin, political opinion, gender or sexual orientation or that compliance with the request/order would cause injury to that person for any of these reasons, or would violate the human rights of a person or the rights of a person under applicable laws.[3]
3. **Situations of conflicts of law, including comity analysis:**
   International agreements should mandate a mechanism to resolve any questions regarding conflicts of laws with other countries when such conflicts arise in connection with requests/orders.

[1] *There is a recognition that larger companies will be better positioned to exercise these rights than will smaller providers.*

[2] *There is a lack of consensus on the specific list of grounds below.*

[3] *There is a lack of consensus on this item.*

CRITERIA D - USERS

1. **Conditions of user notification and secrecy of requests/orders[1]:**
   a. The default rule should be that requesting countries have the duty to provide notification to users at the time that a request/order seeking to obtain their data is issued. The regime should ensure that providers have the right to provide notice to their users. However, notice may be delayed and the request/order may be kept confidential for a limited time period when disclosure would jeopardize an ongoing investigation. Notice should only be delayed for as long as is necessary to protect the investigation.
   b. The regime should provide that when the requesting country seeks secrecy for an order, investigators are required to (1) make their case for secrecy to the independent authority that reviews and approves requests/orders; and (2) present case-specific facts to justify both why the requesting country itself should not be obligated to notify the user and why it must limit the provider's right to notify its customers of the request. The regime should mandate that any nondisclosure order imposed on a provider be narrowly limited in duration and scope, and not constrain the provider's right to speak any more than is necessary to serve law enforcement's demonstrated need for secrecy. The regime should also ensure that providers are permitted to challenge nondisclosure orders to ensure that nondisclosure orders satisfy these requirements.
2. **Access to remedies (suspects and other relevant users) and information about such remedies:**
   The regime should ensure that all users whose data is sought (suspects and other relevant users) have a meaningful opportunity to challenge the transmission and use of their data.
   a. This includes the ability to challenge the request/order on the grounds
      i. that the request/order is overbroad, irrelevant, or abusive, or violates the terms of an international agreement or is otherwise unlawful;
      ii. that the request/order has been made for the purpose of prosecuting or punishing a person on account of that person's race, religion, nationality, ethnic origin, political opinion, gender or sexual orientation;
      iii. that compliance with the request/order would cause injury to that person for any of these reasons, or would violate the international human rights of a person or the rights of a person under applicable law; and/or
      iv. that the users are exercising any other right they may possess under applicable law.
   b. The procedures for such challenges may be provided either through any applicable criminal proceeding in which government authorities seek to use these data, through data protection authorities, or through other available domestic statutory and civil remedies.

CRITERIA E - TRANSPARENCY / ACCOUNTABILITY

1. **Modalities of statistics collection (including information by public authorities) and public availability of such data:**
   a. The relevant legal authority within each country should make available to the public the rules governing cross-border data requests/orders, including the processes to be followed and the standards that apply to assess whether such requests/orders are authorized and legitimate.

b. The relevant legal authority within each country should regularly and periodically publish statistics showing the number of cross-border data requests/orders they issued during the relevant time period, the types of data sought, and the number of requests/orders that resulted in production of data.

c. Providers should regularly and periodically publish statistics showing the number of cross-border data requests/orders they receive, as well as the number of accounts and/or users covered by these requests/orders. In their reports, providers should break out the number of such requests/orders for which they produced data, and the number of such requests/orders that were rejected.

2. Notice:

On a periodic basis, requesting countries should provide notice of data requests/orders to the provider's country (country where the provider's headquarters is located). Notices should contain sufficient information to facilitate accountability by assisting the country receiving the notices to assess compliance with the regime and to determine whether implementing agreements should be renewed. The content of these notices should also be adapted as necessary to protect privacy and confidentiality.[1]

---

[1] *There is a lack of consensus on this item. Some oppose it on principle and others, on the contrary, would like such a notice to the provider's home country to be made simultaneously with to the request to the provider, to help identify potential abuses as they occur.*

PART II - SCALABILITY

CRITERIA F - DIVERSITY OF PUBLIC AUTHORITIES

1. **Administrative structures**
   Regimes must be able to take into account the heterogeneity of possible administrative organizations existing within countries, including in particular the differences between federal and unitary countries.

2. **Authorized initiating authorities**
   Irrespective of the modalities of independent validation and transmission of cross-border requests (see above), requests are initiated by the actors in charge of the investigation, according to national laws and procedures. Given the diversity of domestic organization of competences across jurisdictions, any regime should define what are the authorized levels at which requests can be issued to foreign providers.

3. **Authentication**
   Providers must be able to authenticate the law enforcement agency initiating the request, i.e. to be certain that the requester is indeed who or what it declares it is, in parallel with the relevant criteria determining its right to issue such cross-border requests. This authentication must be a part of the electronic system by which the provider receives the request and can be established in different possible ways[1], including:

   a. Individual pre-registration on companies portals, through for instance the use of a recognizable governmental email account, a statement from a high-ranking law enforcement officer on official letterhead, and/or an order or other official document from a court, judge or other independent agency. This approach has been workable for larger countries and larger companies, which covers the majority of overall requests. This approach may not, however, easily cover all countries or smaller companies.

   b. A system of transmission portals within countries integrating such authentication functionalities.

   c. A specific mechanism established in bilateral agreements (such as envisaged in the US CLOUD Act approach) conferring the authentication authority to a specific entity in the requesting country, which then authorizes the appropriate law enforcement entities to use the transmission system.

   d. A dedicated entity, different from the issuing country or receiving country, accrediting a national authority to handle the national authentication system, or providing authenticated email addresses.

   e. A general, potentially distributed, system of authentication providing individual tokens to pre-registered law enforcement units.

Specific procedures should be established to enable authentication in situations of emergency or time sensitive requests/orders even if the requesting authority has not been pre-authenticated.

Particular attention is required to ensure the security of the authentication system to prevent abuses.

[1] *The list below describes some existing or potential approaches to authentication, but does not prejudge the level of support enjoyed by the different methods.*

CRITERIA G - DIVERSITY OF PROVIDERS

1. **Sizes**
   Small providers may face specific challenges. Irrespective of special provisions that might be applicable to them, they may envisage mutualization efforts to handle requests, including:
   a. Shared local representation for the reception of requests/orders for regimes (such as the proposed EU E-evidence Regulation) that would require it,
   b. The creation of - or subscription to - joint portals preserving separate channels of communication for different providers but leveraging economies of scale.
2. **Types of data**
   Different services store very diverse types of data. Providers can develop dedicated documentation to help public authorities understand what information can be accessible and the corresponding procedures and safeguards.

CRITERIA H - GEOGRAPHIC SCALABILITY

1. **Human rights:**
   Any regime allowing direct cross-border electronic evidence demands by law enforcement to providers should mandate that all participating countries respect and protect international human rights.
2. **Scalability models**
   The three approaches currently envisaged to establish regimes for cross-border requests approach potential geographic scalability to an increasing number of countries in different ways:
   a. The **US CLOUD Act** anticipates the conclusion of successive bilateral executive agreements between the United States and countries it considers as presenting sufficient substantive and procedural guarantees in their legal system. The overall framework will require significant agreement negotiations on a country-by-country basis and only a limited number of countries might meet the required standard in their existing legal framework.
   b. The **EU E-evidence Regulation** currently under discussion in the European Union aims to enable the issuance of compulsory Production Orders under detailed criteria for validity. It is not intended to apply beyond the Union members, but countries in other parts of the world might see in this approach a template that could be replicated at their national or regional level, enabling progressively a form of geographic scalability. However, nothing will ensure that sufficient human rights protections are always incorporated in such regimes, as they will be established unilaterally.
   c. The **Additional Protocol to the Budapest Convention** currently under discussion within the Council of Europe will, like the Convention itself, be open to accession by any country endorsing its provisions. Its scalability model therefore corresponds to the traditional multilateral model of geographic scalability, with all its benefits and potential limitations.
3. **Meeting validation requirements for each request**
   As indicated above, the existing legal framework of particular countries might not meet the high standards expected in a regime for cross-border access to electronic evidence. It is often argued that the inability of such countries to issue cross-border requests even in legitimate situations constitute an incentive to establish mandatory data localization requirements with potentially

detrimental economic and security consequences. In such cases, two avenues at least can be envisaged to remedy this situation:

a. Requesting country uses only certain procedures under its existing laws: The requesting country commits to use only certain procedures in that country's existing law that ensure that sufficient protections are met for the communication of electronic evidence.

   Example: The laws of Country A allow for a warrant to be obtained either by the signature of a law enforcement supervisor or the signature of a judge. Cross-border requests would only be considered valid if approved pursuant to the judge route in Country A's existing law.

b. Requesting country adopts additional provisions applying specifically to cross-border requests.

   Example: Country A's laws may provide for approval by a judge only after a warrant issued by a law enforcement supervisor has not been successful in obtaining the evidence sought. A minor change to the country's law would permit the use of the judge route for cross-border requests.

Such approaches could apply both in the context of bilateral agreements under the US CLOUD Act or in any effort to implement a domestic regime inspired by the EU E-evidence proposed framework. Yet, this only addresses the specific issue of the introduction of a judicial validation when the existing legal system does not always require it for domestic requests and not other potential limitations in countries' existing legal frameworks.

PART III - REQUESTS / ORDERS STANDARDS

In addition to the regime provisions regarding degree of independent validation, standard of proof, necessity and proportionality (as described in Criteria B - Public Authorities), the following elements should be taken into account regarding individual requests/orders.

CRITERIA I - TRANSMISSION

1. **Secure channels and traceability**
   Data requests/orders should be transmitted to providers securely, following best practices for data security such as end-to-end encryption. The system for transmitting requests/orders should be traceable, to enable providers and users to assess the authenticity of requests/orders and to permit regular audits.
2. **Transmitting authorities**
   Countries should limit[1] the number of Points of Contact (POCs) that are authorized to transmit data requests/orders, in order to ensure the quality of requests/orders and to assist providers to verify the authenticity of requests/orders.
3. **Certification**
   Transmitting POCs may perform in addition some non-substantive verification of requests/orders regarding completeness and conformity with the procedural requirements of the specific regime under which requests/orders are issued.
4. **Recipient identification (POC or Representative)**
   The number of POCs per provider should be limited to simplify authentication, but providers should be permitted to have more than one POC as needed. Providers should disclose POCs to countries that need them and keep them updated.

[1] *There is a lack of consensus on this item. Some fear that this would create transmission bottlenecks, and would only envisage it if requests/orders were automatically transmitted and processed.*

CRITERIA J - REQUEST FORMATS

1. **Written form**
   All cross-border data requests/orders issued to providers should be in writing, including via electronic means, even in emergencies.
2. **Language**
   Requests/orders should be sent in the language of the requesting country, and where needed to ensure that the provider's personnel can understand the request/order, should also be translated into a primary language spoken in the provider's country.

3. Request components and formats[1]

CLUSTER	LABEL	DESCRIPTION
REFERENCING	**Request Number**	Request ID number that identifies the specific demand; used for reference tracking and potential audits.
	Time	Timestamp on emission from requesting country.
	Issuing Country	Indicates the country of origin of the demand.
	Recipient Company	Indicates the destination of the demand, in particular a Point of Entry (POE).
	Case Number	Identifies the corresponding legal case in the requesting country.
STATUS	**Request Status**	Identifies whether the demand is new or a follow up to a previous MLA or preservation order.
	Previous Preservation or MLA Requests / Orders	Information regarding any previous preservation request/order or MLA request.
	Case Status	Identifies status and progress of the case in the requesting country, at the time of request (e.g. pre-trial, trial, crime in progress, ...).
DATA SOUGHT	**Account information**	Identifies the specific target of the request: specific IP address, domain name, URL, user identifiers or accounts (criteria of specificity).
	Data requested	The specific user data being requested, with the highest degree of precision.
	Time Range/Period	The time period covered by the request/ order for which the data is being demanded.
TIMING	**Deadline**	Identifies specific deadlines attached with the demand.
	Emergency	Identifies whether the circumstances have a character of urgency.
	Rationale for Emergency	Justification of the emergency (e.g. its nature, link of the request to the emergency, how it can avert the emergency).
CONFIDENTIALITY	**Confidentiality**	Specifies whether specific circumstances justify that some parts or all of the demand not be communicated to the concerned user.
	Rationale for Confidentiality	Justification of non-notification.
	Confidentiality timeline	Duration of the confidentiality exception.

[1] *This list of components was identified on the basis of different templates and formats elaborated in the context of inter alia the EU E-evidence proposal, the Council of Europe T-CY, as well as a joint study by UNCTED, UNODC and IAP.*

CLUSTER	LABEL	DESCRIPTION
CASE	**Offense**	Description of the alleged offense.
	Legal Basis	National legal framework upon which this demand is based; an explicit link to an online version in English of the corresponding law/jurisprudence could be a requirement for validity/acceptability of the demand.
	Summary of the Case	Facts, relation with the data, purpose and necessity, charges pressed/list of offenses.
	International regime	Framework under which the cross-border request is issued.
AUTHORITIES	**Issuing Authority**	The authority and/or POC that has issued the demand and its details.
	Validating Authority	The authority that has validated the demand in the requesting country and its details.
	Investigating / Prosecuting authority	Details of the authority investigating or prosecuting the case in the requesting country.
CONTACTS	**Response Notification**	Contact details in the requesting country to which response notifications should be directed to.
	Reception of data	Details of the authority in the requesting country to which user/suspect information should be transferred to.
	Contact Information	Point of Contact in requesting country that will be the focal point for follow up questions or additional information.
CERTIFICATION	**Certification**	Self-certification by the issuing authority.
SIGNATURE	**Signature**	Identifies the signature and/or stamp of the validating authority.
OTHER		

The table below and the asterisks therein are non-exhaustive suggestions on how the corresponding items could be used. No prescriptive or normative conclusions should be drawn by the presence or absence of an asterisk in any cell.

Cluster		Label	Necessary for Technical Management	Useful for Transparency Reporting	Relevant to Determine Response(s) (substantive)	Decisive for the Validity of Requests or Orders (procedural)
Referencing	1.1	Request Number				
	1.2	Time				
	1.3	Issuing Country	x	x		x
	1.4	Recipient Company	x	x	x	
Status	2.1	Request Status				
	2.2	Previous Preservation or MLA Request/Orders	x			
	2.3	Case Status				
Data Sought	3.1	Account Information	x		x	
	3.2	Data Requested	x			x
	3.4	Time Range/Period	x		x	
Timing	4.1	Deadline	x			
	4.2	Emergency	x	x	x	
	4.3	Rationale for Emergency			x	
	4.4	Time Sensitivity	x	x	x	
	4.5	Rationale for Time Sensitivity			x	
Confidentiality	5.1	Confidentiality	x	x	x	
	5.2	Rationale for Confidentiality			x	
	5.3	Confidentiality Timeline	x			
Case	6.1	Offence		x	x	
	6.2	Legal Basis		x	x	
	6.3	Summary of Case			x	
	6.4	Case Number				
	6.5	Sanction Level			x	
	6.6	International Regime		x	x	x
Authorities	7.1	Issuing Authority				x
	7.2	Validating Authority				x
	7.3	Investigating/Prosecuting Authority				x
Contacts	8.1	Response Notification	x			
	8.2	Reception of data	x			
	8.3	Contact Information	x			x
Certification	9.1	Certification				x
Signature	10.1	Signature				x

CRITERIA K - NEXUS

1. **Substantial connection**

   Location of a crime in a country's territory is generally accepted as, and remains the primary criterion determining its right to investigate, and the national rules, procedures and criteria to determine the location of physical crimes are well established.

   However, regarding crimes involving the use of digital means, determining the location of crime is often more complex, having to take into account other factors such as the location of the suspect(s) at the time the crime is committed, and/or the location of the victim(s).

   In establishing the right to investigate, national rules and procedures may also take into account:

   a. The location of the harm, while being mindful of the risk of creating de facto universal jurisdiction over crimes with very distributed harm;

   b. The nationality of the suspect(s) and the victim(s), as it is a generally accepted principle of public international law that states can protect their nationals, and can investigate acts by their nationals.

2. **Legitimate interest in obtaining the specific data sought**

   In the context of a particular regime for cross-border access to electronic evidence, public authorities issuing an individual request/order justify their legitimate interest in the specific data sought when:

   a. The investigated crime is within the scope of the country's criminal laws, and the requested access is within the scope of the public authorities' legal investigatory power;

   b. The investigated crime is within the scope of the regime, taking into account potential penalties thresholds in relation to the type of data sought;

   c. The regime's standard of proof is met (see Criteria B - Public Authorities, point 2 - "Standard of proof");

   d. They can demonstrate that the same information cannot be obtained through other means.

3. **Interests of others**

   a. The following factors can help requesting authorities identify, at the start of their procedure or in the course of it, the potential interests of other actors:

      i. The rights, in particular privacy rights, of the suspect, victim, and any other party whose data will be accessed, according to their nationality or residence, as soon as it is known;

      ii. The risk of imposing duties on a party that conflict with the duties or rights that party holds under applicable foreign law;

      iii. The likelihood that the investigative measure might impact ongoing investigations in another State;

      iv. The potential multiplicity of countries affected by the crime, to ensure the respect of the rule "*ne bis in idem*".

   b. On this basis, and within the provisions of the relevant direct access regime, the requesting authority can evaluate its appropriate interaction with countries:

      i. Whose nationals or residents are targeted by the request/order for data;

      ii. Where the data controller is located, if applicable.

   c. Such interaction can include:

      i. Refraining from issuing the request/order;

      ii. Notifying the relevant State;

iii. Allowing another State to take the lead in investigations;

iv. Coordinating with one or several States in the investigation;

v. Mechanisms, including comity analysis, to avoid conflict of laws with third countries and resolve such conflicts should they arise.

OPERATIONAL MECHANISM

MARK-UP LANGUAGE AND INTEROPERABILITY TAGS

CONTEXT

Data stored by foreign-based service providers now constitutes essential evidence for a growing proportion of criminal investigations. Due to constraints in the traditional ways to obtain this data, in particular via Mutual Legal Assistance Treaties (MLATs), public authorities increasingly send cross-border requests directly to these foreign providers, for both preservation and production of this information.

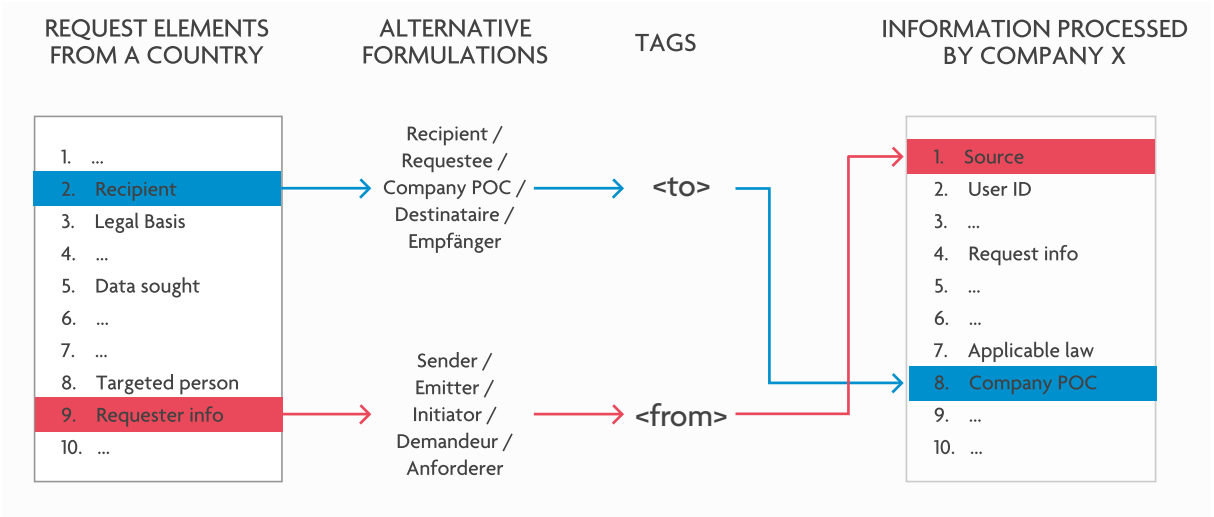
Various public authorities have developed or are developing their own forms for such requests. Some have proprietary filing systems to produce them. At the same time, the largest providers develop their own elaborate portals for request submission, while smaller providers have mere abuse Points of Contact (POCs). Some authorities find this heterogeneity inefficient, because it may lead to duplications in the entering of information and an obligation to learn numerous procedures.

Yet, full standardization of requests formats and submission mechanisms would be difficult. It is also not desired by the different actors, who are attached to their respective practices. But harmonization is not necessary: an approach aiming at interoperability has more potential.

Indeed, analysis of different request formats (existing or proposed) shows significant commonality. Though sections labels and their order might differ, they are largely similar in substance: information on the requester and requestee, the request's legal basis, the procedure followed, the specific data sought, or rationale for emergency, to name a few. Mapping these common elements in the way suggested below can enable interoperability among actors with significant benefits for all.

THE IDEA OF A MARK-UP LANGUAGE

On the Web, HTML tags annotate the key elements of a particular text on a server, allowing the user's browser to display the page accurately after transmission. By rough analogy, a shared set of tags could help identify and encode the various typical components of data access requests. This would enable clear communication between actors, irrespective of how requests were prepared or will be handled, of the labels used on both sides, or even the language used, as illustrated in these simple examples:



Implementation of this markup language is meant to be voluntary. Its capacity to foster efficiency and interoperability should nonetheless encourage broad progressive adoption. Furthermore, the cooperative development and regular updating by public authorities, companies and other relevant actors of this set of tags should also foster greater trust among them.

OPERATIONAL BENEFITS

The existence of such an interoperability standard would provide the following additional benefits in terms of:

- **End-to-end neutrality** - The approach is neutral vis-a-vis any transmission system already employed or to be developed;
- **Flexibility** - It accommodates different structure and ordering of request components by the different actors;
- **Easy implementation** - Requesters and recipients who already have developed their own systems can continue to use them and only need to develop simple format converters;
- **Scalability** - Small public authorities and private actors can easily develop tools (or use some developed by third-party actors) to produce or manage quality requests;
- **Due process** - the existence of such structured requests will facilitate the evaluation of their completeness and their conformity to any regime-agreed quality standard;
- **Workflow** - A receiving company can automatically sort and distribute request parts to its relevant services, e.g.: legal basis information to its legal department and info on data sought to its operational one. This fosters both efficiency and confidentiality;
- **Security** - Sensitive parts of requests can be distinguished and encrypted;
- **Transparency** - Top-level statistical information can be easily separated and collected, simplifying reporting;
- **Versatility** - Tags allow an easy mapping to labels in various languages.

As a final note, although currently explored for direct requests, such a set of tags could also be useful in the context of MLA requests and other government-to-government interactions.

NEXT STEPS

The 3rd Global Conference of the Internet & Jurisdiction Policy Network in Berlin can discuss the validity of this proposal, the potential mandate and timeline of such a group, as well as ways to ensure involvement of the most relevant stakeholders.