

CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE

MARCH 2021 I&JPN REF: 21-103

www.internetjurisdiction.net/data/toolkit



The Internet & Jurisdiction Policy Network is the multistakeholder organization fostering legal interoperability in cyberspace. Its stakeholders 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 400 key entities from six stakeholder groups around the world including: governments, the world's largest internet companies, the technical community, civil society groups, leading universities and international organizations.

DESIGN & LAYOUT

João Pascoal Studio

www.joaopascoal.com

CITATION

Internet & Jurisdicion Policy Network Toolkit Cross-border Access to Electroninc Evidence (2021)



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

TABLE OF CONTENTS

1.	ISSUE FRAMING	04
2.	I&JPN METHODOLOGY	06
3.	TOOLKIT: CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE	09
3.1	GENERAL STRUCTURE AND KEY REGIME COMPONENTS FOR ACCESSING ELECTRONIC EVIDENCE	11
	CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE GENERAL REGIME ARCHITECTURE	12
	REGIME STANDARDS	15
	> Regime Scope	16
	> Public Authorities	17
	> Providers	18
	> Users	19
	REQUEST/ORDER STANDARDS	20
	> Transmission	21
	> Request Formats	22
	> Nexus	26
3.2	VOLUNTARY DISCLOSURE	28
	REGIME STANDARDS	29
	 Cross-Border Requests for Voluntary Disclosure of Subscriber Information, including Annex. 	30
	REQUEST/ORDER STANDARDS	34
	> Request Components for Access to Subscriber Information Under Voluntary Disclosure Regime	
4.	ABOUT THE INTERNET & JURISDICTION POLICY NETWORK	37
5.	ACKNOWI FDGMFNTS	39

1. ISSUE FRAMING

Criminal investigations increasingly require access to information about users and digital evidence stored in the cloud by private companies in jurisdictions outside the requesting country.

Existing Mutual Legal Assistance Treaties (MLATs) procedures are broadly recognized as slow and ill-adapted. Meanwhile, limited procedural guarantees apply to direct requests sent to companies, and such direct requests can even be forbidden by some national blocking statutes.

This situation of legal uncertainty is not sustainable. In particular, the lack of clear cooperation frameworks encourages mandatory data localization approaches that are technically difficult to implement and can have detrimental impacts on the cloud economy and human rights.

Different efforts are under way to develop solutions and policy coherence between them is important: uncoordinated actions can have unintended consequences or increase conflicts of laws.

All actors are confronted with a common challenge: developing policy standards respecting privacy and due process that define the conditions under which authorized law enforcement authorities can request from foreign entities access to stored user data necessary for lawful investigations.

Towards this the Data & Jurisdiction Program Contact Group focuses on the definition of high substantive and procedural standards

- Allowing relevant authorities from specific countries
- > In investigations regarding certain types of crimes with a 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 use of existing MLAT procedures poses an additional layer of complexity. They can impose on requests by one country, the laws of another that often has no connection with the underlying investigation other than the location of the provider. Frequently, the victim(s) and the suspect(s) are both located in the requesting country.

To alleviate this imbalance, innovative frameworks have to be developed to allow law enforcement authorities to make requests directly to foreign-based service providers. Towards ensuring the protection of users' rights, such frameworks must clearly define their scope and the applicable legal standards and procedures, while also ensuring high due process safeguards.

Simultaneously, these frameworks have to also contend with the identification of potential conflicts of laws across the different jurisdictions involved, and to prescribe innovative mechanisms to fairly distribute the burden of addressing these conflicts and of safeguarding users' rights and interests.

As more mechanisms for cross-border access to electronic evidence take root around the world in different forms, there is a risk of proliferation of uncoordinated and haphazard actions, without sufficient regard for international human rights standards and due process guarantees. In the absence of sufficiently global frameworks, a potential legal arms race calling for mandatory data localization requirements may result in fragmentation of the internet.

In parallel with the development of appropriate frameworks, existing voluntary disclosure mechanisms, in spite of their limited scope, can be further improved by establishing due process standards for requests, as well defining channels of communications and procedures that help set mutual expectations among actors.

The Data & Jurisdiction Program Contact Group, consisting of experts from governments, internet companies, technical operators, civil society, leading universities and international organizations has, over the years, identified the key issues that structure new approaches to inform the debate on cross-border access to electronic evidence.



2. I&JPN METHODOLOGY

The Internet & Jurisdiction Policy Network fosters a new approach to transnational policy-making. Its innovative methodology identifies relevant stakeholders to define common problems and produce solutions to pressing and complex policy challenges. The neutral and replicable approach, structures interactions among diverse policy actors who would normally not have the opportunity to work together on practical and concrete outcomes.

In regular iterations since 2016, the Data & Jurisdiction Program Contact Group engages a select set of these global policy actors while trying to ensure balanced geographical representation from governments, internet companies, technical operators, civil society, leading universities and international organizations. Using the I&JPN Methodology, Contact Groups have iteratively developed concrete outcomes pertaining to specific facets of cross-border access to electronic evidence. Based on this methodology, future Contact Groups will continue to develop specific policy outcomes on focused issues while also addressing emerging challenges.

The Internet &
Jurisdiction Policy
Network fosters a
new approach to
transnational policymaking. Its innovative
methodology
identifies relevant
stakeholders to
define common
problems and
produce solutions to
pressing and complex
policy challenges.

Meet the Members of the Data & Jurisdiction Contact Group from 2018 - 2020 <u>here</u>





FRAMING COMMON PROBLEMS

Issues can best be addressed when formulated as problems that stakeholders have in common rather than with one another. As a first step stakeholders are consulted to develop a shared framing of the issue at hand and build a shared vernacular. This helps develop a common understanding of the policy problem and helps identify key areas for cooperation where stakeholders can work collaboratively to develop practical and operational solutions.



How can transnational data flows and the protection of privacy be reconciled with lawful access requirements to address crime?

I&JPN Data & Jurisdiction Framing Paper (2017)ⁱ



SETTING COMMON OBJECTIVES

Based on these areas of cooperation, a dedicated Contact Group, guided by a neutral and independent coordinator, identifies key structuring questions that guide discussions among stakeholders and provide a framework within which concrete policy solutions can be developed. These discussions documented as Policy Options define common objectives to ensure better policy coherence and structure further work.



This document aims at providing, in a forward-looking approach, guiding elements to structure further discussion on possible frameworks regarding cross-border access to electronic evidence. It documents the key substantive and procedural dimensions that can help overcome divergences.

I&JPN Data & Jurisdiction Policy Options (2018)ii



DEVELOPING COMMON APPROACHES

Based on the objectives identified, intense work in the Contact Group aims to develop scalable, interoperable policy solutions. These can take the form of Operational Norms – to help actors organize their own behavior and mutual interactions; Operational Criteria – to guide actors who develop, evaluate & implement solutions; and Operational Mechanisms – that offer concrete avenues for cooperation.



The work of the dedicated Contact Group of the Internet & Jurisdiction Policy Network aims to contribute to this discussion by developing common policy approaches for crossborder access to electronic evidence.

I&JPN Data & Jurisdiction Operational Approaches (2019)ⁱⁱⁱ



FOSTERING LEGAL INTEROPERABILITY

Further work is conducted to evangelize, communicate and aid the implementation of these policy solutions. This may take the form of Toolkits compiling thematic Outcomes developed by the Contact Group. This helps further legal interoperability in two dimensions:

- > Interoperability between actors: to enable automation of the technical workflow among public authorities and private actors across borders to ensure due process at scale.
- > Interoperability between norms: to reduce the potential of conflicts in rule-setting, implementation and enforcement among different regimes.
- i. https://www.internetjurisdiction.net/uploads/pdfs/Papers/Data-Jurisdiction-Program-Paper.pdf
- ii. https://www.internetjurisdiction.net/uploads/pdfs/Papers/Data-Jurisdiction-Policy-Options-Document.pdf
- iii. https://www.internetjurisdiction.net/uploads/pdfs/Papers/Data-Jurisdiction-Program-Operational-Approaches.pdf

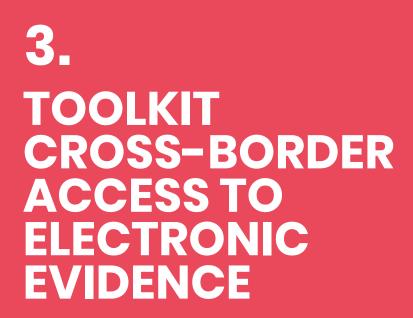


The Toolkit on Cross-border Access to Electronic Evidence provides resources covering two dimensions:

- 1) A general framework regarding the modalities of access to cross-border electronic evidence, its challenges and the necessary safeguards for protecting rights of users.
- 2) Concrete tools that inform and improve the technical interfacing between actors through request formats that can improve communications. This Toolkit seeks to improve the interactions between actors while identifying and recommending appropriate due-process guarantees at different stages that can be applied to requests or orders for cross-border electronic evidence. The Data & Jurisdiction Program Contact Group will continue to engage on the topics addressed in the Toolkit with the objective of refining them and developing new tools.

The subsequent components of this Toolkit 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. They are a best effort by the Members of each Contact Group to address the important cross-border issues pertaining to access to electronic evidence that have been curated by the Secretariat of the Internet & Jurisdiction Policy Network into the framework of this Toolkit.

This Toolkit seeks
to improve the
interactions between
actors while identifying
and recommending
appropriate due-process
guarantees at different
stages that can be applied
to requests or orders for
cross-border electronic
evidence.



STRUCTURE

GENERAL STRUCTURE AND KEY REGIME COMPONENTS FOR ACCESSING ELECTRONIC EVIDENCE

VOLUNTARY DISCLOSURE



STRUCTURE

This Toolkit curates resources that can provide actors with clarity on their respective roles and responsibilities in the process of cross-border access to electronic evidence. While providing practical tools for law enforcement agencies and service providers to understand the different components of and thresholds for cross-border requests, this Toolkit also seeks to inform the debate surrounding multilateral, and bilateral international agreements facilitating such access.

This Toolkit has a twofold structure. The first section provides an overview of the architecture and components of any cross-border regime for electronic evidence and aims to serve as an analytical framework for navigating the complexities of such regimes. The second section of this Toolkit adapts these components to suit the parameters of voluntary disclosure, in order to provide context and tools for states and providers to improve the process of, respectively, making and handling such requests.



REGIME STANDARDS CROSS-BORDER REQUESTS FOR VOLUNTARY DISCLOSURE OF SUBSCRIBER INFORMATION, INCLUDING ANNEX REQUEST/ORDER STANDARDS REQUEST COMPONENTS FOR ACCESS TO SUBSCRIBER INFORMATION UNDER VOLUNTARY DISCLOSURE REGIME

3.1

GENERAL STRUCTURE AND KEY REGIME COMPONENTS FOR ACCESSING ELECTRONIC EVIDENCE

This part of the Toolkit identifies a set of **core components** that need to be defined according to the parameters of any regime facilitating cross-border access to electronic evidence. This section consists of:

- A presentation of the general set of components (and definitions thereof) that make up any given regime for crossborder access to electronic evidence. This can also be used as a common grid of analysis.
- Baseline multistakeholder benchmarks for the scope of any such regime (Regime Standards).
- The definition of applicable benchmarks concerning the modalities of issuance of requests within a regime (Request/ Order Standards).



CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE GENERAL REGIME ARCHITECTURE

1&JPN REF. 20-111

CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE GENERAL REGIME ARCHITECTURE

All regimes for cross-border access to electronic evidence naturally follow a similar architecture. In order to reconcile high substantive and procedural guarantees with efficiency, a corresponding set of basic regime components was identified by a dedicated Contact Group¹ of the Internet & Jurisdiction Policy Network in 2018–19. The present document lists and provides definitions for these components, as a companion to the **Operational Approaches**² released by this Group in April 2019, which documented the degree of convergence among diverse actors on possible standards for each component. These two documents provide all actors with a common grid of analysis in the context of ongoing debates around cross-border access to electronic evidence regimes.

Regime Scope

Data Covered

Definition of the types of user data the regime intends to enable access to. Each category will determine specific procedural safeguards. The most frequent categories are: subscriber information, traffic data, and content data, albeit with some variability regarding what they precisely entail in each regime, as well as variability among providers.

Types of Crimes covered

Identification of the criminal offenses for which the regime procedures can be used. This can entail, for instance, thresholds regarding the minimum sanction incurred.

Providers Covered

Identification, if any, of the required degree of connection of the provider to the issuing State (e.g. "providing services"), and corresponding factors.

Requesting State

Judicial/Independent Validation

Type of judicial/independent validation that would be required for each request or order from the Requesting State. Some regimes, however, may only envisage general oversight of the process rather than order-by-order validation.

Standard of Proof

Threshold of factual elements that have to be provided to justify relevance of the data requested to the case.

INTERNET & JURISDICTION POLICY NETWORK

^{1.} Data & Jurisdiction Contact Group 2018-2019

 $[\]textbf{2.} \ \text{https://www.internetjurisdiction.net/uploads/pdfs/Papers/Data-Jurisdiction-Program-Operational-Approaches.pdf} \\$

Necessity and Proportionality

Explicit mention that requests/orders must respect necessity and proportionality principles.

Authorized Authorities

Criteria, if any in the regime, for what administrative levels with competence to investigate³ under local laws are allowed to initiate, issue or transmit a request or an order.

Providers

Clarification of Requests/Orders

Definition of the conditions under which a service provider can request additional information from the issuing authority, regarding imprecise, incomplete or insufficiently documented requests/orders.

Challenge of Requests/Orders

Conditions, if any, under which a service provider can object to or refuse to execute a request/order.

Conflicts of Laws

Specific mechanisms (including comity analysis) to address situations where a service provider can be caught between competing and conflicting legal obligations.

Response Time

Expected response time by the provider to a properly submitted request/order.

Users

Conditions of User Notification and Secrecy of Requests/Orders

Under what modalities authorities and/or service providers should inform the targeted user to ensure the capacity of recourse and conditions under which such information can potentially be delayed.

Access to Legal and Administrative Remedies

Procedures and grounds under which users can challenge the disclosure and/or use of their data.

Other States

With Connection to the Provider

Modalities, if any, of information to a country where the provider is incorporated, has a relevant subsidiary or its legal representation, for any request/order, and/or on a periodic basis.

With Connection to the Suspect or Victim

Modalities, if any, of information to a country where the suspect or victim is a citizen, permanent resident or was present on the occasion of the investigated crime.

^{3.} Includes, inter alia, the valid legal basis, substantial connection to the crime and legitimate interest to the data sought.



REGIME STANDARDS

I&JPN REF. 19-104

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 crimes4; and
- b. Where the detection, investigation and/or prosecution does not infringe on international human rights.⁵



^{4.} 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.

^{5.} The Contact 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.

I&JPN RFF, 19-105

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 person⁶ 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 require 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.

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.

6. Some members of the Contact 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.

INTERNET & JURISDICTION POLICY NETWORK

I&JPN RFF, 19-106

PROVIDERS

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/order⁷ on the ground⁸ 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.9

3. Situations of conflicts of laws, 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.

^{7.} There is a recognition that larger companies will be better positioned to exercise these rights than will smaller providers.

^{8.} There is a lack of consensus on the specific list of grounds below.

^{9.} There is a lack of consensus on this item.

USERS

1. Conditions of user notification and secrecy of requests/orders10:

- 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.

INTERNET & JURISDICTION POLICY NETWORK

^{10.} 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 the request to the provider, to help identify potential abuses as they occur.



REQUEST/ORDER STANDARDS

I&JPN RFF, 19-112

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 limit¹¹ 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.

INTERNET & JURISDICTION POLICY NETWORK

^{11.} 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.

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 formats¹²

CLUSTER	LABEL	DESCRIPTION		
	Request Number	Request ID number that identifies the specific demand; used for reference tracking and potential audits.		
	Time	Timestamp on emission from requesting country.		
REFERENCING	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.		
	Request Status	Identifies whether the demand is new or a follow up to a previous MLA or preservation order.		
STATUS	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,).		

^{12.} 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.

INTERNET & JURISDICTION POLICY NETWORK

	Account information	Identifies the specific target of the request: specific IP address, domain name, URL, user identifiers or accounts (criteria of specificity).
DATA SOUGHT	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.
	Deadline	Identifies specific deadlines attached with the demand.
TIMING	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	Specifies whether specific circumstances justify that some parts or all of the demand not be communicated to the concerned user.
CONFIDENTIALITY	Rationale for Confidentiality	Justification of non-notification.
	Confidentiality timeline	Duration of the confidentiality exception.
	Offense	Description of the alleged offense.
CASE	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.
	Issuing Authority	The authority and/or POC that has issued the demand and its details.
AUTHORITIES	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.
	Response Notification	Contact details in the requesting country to which response notifications should be directed to.
CONTACTS	Reception of data	Details of the authority in the requesting country to which user/ suspect information should be transferred.
	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)
	1.1	Request Number				
	1.2	Time				
REFERENCING	1.3	Issuing Country	Х	Х		Х
	1.4	Recipient Company	Х	Х	Х	
	1.5	Case Number				
	2.1	Request Status				
STATUS	2.2	Previous Preservation or MLA Requests/Orders	х			
	2.3	Case Status				
	3.1	Account Information	Х		Х	
DATA SOUGHT	3.2	Data Requested	Х			Х
	3.4	Time Range/Period	Х		Х	
	4.1	Deadline	Х			
TIMING	4.2	Emergency	х	Х	Х	
	4.3	Rationale for Emergency			Х	
	5.1	Confidentiality	х	х	Х	
CONFIDENTIALITY	5.2	Rationale for Confidentiality			Х	
	5.3	Confidentiality Timeline	X			

	6.1	Offence		х	Х	
	6.2	Legal Basis		Х	Х	
CASE	6.3	Summary of Case			Х	
	6.4	International Regime		Х	Х	Х
	7.1	Issuing Authority				х
AUTHORITIES	7.2	Validating Authority				Х
	7.3	Investigating/ Prosecuting Authority				х
	8.1	Response Notification	х			
CONTACTS	8.2	Reception of data	Х			
	8.3	Contact Information	Х			Х
CERTIFICATION	9.1	Certification				x
SIGNATURE	10.1	Signature				Х

18 JPN RFF, 19-114

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 the 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 point 2 of Public Authorities, under Regime Standards for General Regime Architecture);
- 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:
 - 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:
 - 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:
 - 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 conflicts of laws with third countries and resolve such conflicts should they arise.



3.2

VOLUNTARY DISCLOSURE

This section of the Toolkit focuses on structuring interactions between actors within the context of voluntary disclosure practices followed by service providers in jurisdictions that do not explicitly prohibit them. It provides context and guidance to improve the actionability of requests issued under voluntary disclosure through:

- Setting and managing expectations by adapting the general regime cursors for the purpose of voluntary disclosure (Regime Standards).
- Identifying minimum components of request formats that can be used in the transmission of such requests to service providers (Request/Order Standards).



REGIME STANDARDS

I&JPN REF: 21-102

CROSS-BORDER REQUESTS FOR VOLUNTARY DISCLOSURE OF SUBSCRIBER INFORMATION

Subscriber information¹³ collected by service providers is often useful at various stages of criminal investigations, in particular to identify suspects or victims. Some countries allow service providers incorporated on their territory to voluntarily disclose such information upon requests addressed directly to them by foreign investigating authorities. A similar approach may also be possible with providers based in countries which do not explicitly prohibit such disclosure.

Voluntary disclosure does not replace disclosure under Mutual Legal Assistance Treaties, but may reduce the burden on such instruments by providing a faster avenue for obtaining this specific type of user information.

However, service providers are not expected to know the applicable national laws and procedures¹⁴ of the requesting states that govern issuance of requests for subscriber information. Similarly, requesting states may lack knowledge pertaining to the modalities of communication with service providers in that regard. For these reasons many requests, even when legitimate, may be incomplete or unactionable. Similarly, uncertainty may exist regarding the extent to which the requesting state has abided by the applicable laws and procedures. Cross-border requests must also take into account potentially different definitions of subscriber information across jurisdictions¹⁵, and the type of services the provider offers.

The Internet & Jurisdiction Policy Network has previously documented¹⁶ the general components pertaining to any regime for cross-border access to electronic evidence. Building on this basis, the present document identifies the elements relevant to the specific case of voluntary disclosure of subscriber information. Separate complementary documents¹⁷ provide more detail on implementing some of these components.

This document is intended to help improve the interactions of the respective actors, particularly small ones, in order to inform the issuance by states and handling by service providers of such requests. This may increase the likelihood of obtaining information considered subscriber information in the United States, where major service providers are incorporated.

This document is naturally without prejudice to the outcomes of multilateral or bilateral binding international treaties (such as the Second Additional Protocol to the Budapest Convention or agreements under the US CLOUD Act) and regional frameworks (such as the E-evidence regulation in the European Union).

^{13.} User information stored by service providers are classically categorized as subscriber information, traffic data, or content data. The definition of accessible subscriber information may vary across countries of incorporation.

^{14.} These procedures may naturally vary from state to state.

^{15.} A compilation of the two main definitions of Subscriber Information (United States 18 U.S. Code § 2703 and Council of Europe Budapest Convention - 2nd Additional Protocol) can be found in the Annex of this document.

^{16.} I&JPN Outcome: Cross-Border Access to Electronic Evidence General Regime Architecture

^{17.} www.internetjurisdiction.net/data/toolkit

This document offers a list of suggestions that aim to help requesting states formulate and service providers evaluate voluntary disclosure requests and does not define and set harmonized legal standards across jurisdictions.

SCOPE

Data Covered

Requests made to obtain subscriber information stored¹⁸ by a foreign service provider incorporated in a country that does not prohibit voluntary disclosure of such information.

Types of Crimes Covered¹⁹

Requests made for any crime investigated in the requesting state. However, every request should include a clear reference to the existing legal basis for the investigated crime in the relevant laws of the requesting state.

Service Providers Covered
 Requests made to any digital service accessible in the requesting state.

REQUESTING STATE

Judicial or other Independent Validation

National laws of the requesting state determine the procedures for subscriber information disclosure requests. Given that the primary use of subscriber information is for identification of victims and suspects, laws in the requesting state may not necessarily mandate independent validation for such requests. If judicial or other independent validation is not required by these national laws, the existence of, and a record of compliance with, an independent oversight mechanism (ex-ante or at minimum post-facto review) may help build confidence on the part of the service provider.

Standard of Proof

For every request, the requesting state should provide legal and factual elements demonstrating that the subscriber information sought is relevant to the criminal investigation and that the request meets the substantive and procedural standards for issuance to a domestic service provider. These standards should be consistent with international standards on the rule of law and international human rights.

Necessity and Proportionality

Every request should meet the standard of review for necessity and proportionality under international human rights law, including adequate protection for privacy and other human rights, and international standards for the rule of law.

Authorized Authorities

Authorities with established competence to investigate according to their local legislation initiate a request. The requesting state should verify completeness of every request before transmission. It should also publish regular statistics as part of its transparency commitments. Requesting states should transmit these requests through a limited number of point(s) of contact.

^{18.} This document does not address real-time interception of electronic communications.

^{19.} This document does not cover emergency situations. The Contact Group may address this topic in the future.

SERVICE PROVIDERS

> Clarification of Requests

The service provider is entitled to ask for clarification(s) from the requesting state, e.g., if the request is imprecise, incomplete or insufficiently documented.

- > Evaluation of Requests
 - Service providers should adopt procedures to reduce the risk of the disclosure of subscriber information that could result in a deprivation of rights. They are also encouraged to apply heightened scrutiny according to the human rights records of the requesting state.²⁰
- Declining of Requests

Nothing compels service providers to disclose information in response to such requests. Service providers should notify the requesting state of their decision. They are also encouraged to provide a justification or explanation thereof.

Response Time

Service providers are encouraged to acknowledge the receipt of a request. They are also encouraged to provide an estimate on average response time.

USERS

- User Notification and Secrecy of Requests
 - User notification is essential for users to protect their rights and access to remedies. User notification by the service provider depends on the provider's terms of service, and laws that are applicable to the service provider. If the requesting state, under its national laws, requests the service provider to not notify the user of the request, it should provide a duly justified and time-bound request for secrecy, based on an assessment of the risk of jeopardizing an ongoing investigation. The requesting state should notify the data subject as early as possible, in accordance with applicable national law. If a service provider provides notice to its users, it should do so within a reasonable time. The service provider is encouraged to inform the requesting state, prior to any data disclosure, of the service provider's commitment to notify users of such data disclosure. The requesting state is encouraged to indicate in the request whether it should be deemed withdrawn if the service provider were to notify the user of any disclosure in response to that request.
- Access to judicial or administrative remedies
 - The requesting state should provide, directly to the data subjects, information regarding their access to judicial or, when applicable, administrative remedies. If applicable, service providers may inform users on potential avenues to challenge the disclosure in the country of incorporation of the service provider.

^{20.} Service providers can consult human rights groups and human rights reports to identify those countries.

^{21.} Some Members of the Contact Group express that such requests for secrecy should be approved by a judicial or other independent oversight mechanism.

^{22.} National laws may prescribe such notification at different times, including when the data subject is under investigation, indicted or put on trial.

ANNEX: COMPILATION OF SUBSCRIBER INFORMATION DEFINITIONS

DEFINITIONS:

1) United States

18 U.S. Code § 2703.

Required disclosure of customer communications or records

- (c) Records Concerning Electronic Communication Service or Remote Computing Service.—
 - (2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—
 - (A) name:
 - (B) address;
 - (C) local and long distance telephone connection records, or records of session times and durations;
 - (D) length of service (including start date) and types of service utilized;
 - (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
 - (F) means and source of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

2) Budapest Convention 2nd Additional Protocol

Article 18(3) of the Budapest Convention

For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

- A. the type of communication service used, the technical provisions taken thereto and the period of service;
- B. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
- C. any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

UNITED STATES	COUNCIL OF EUROPE
18 U.S.C. § 2703	Budapest Convention 2 nd Additional Protocol (and Art. 18 of the Budapest Convention)
name, address, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address;	the subscriber's identity, postal or geographic address, telephone and other access number, available on the basis of the service agreement or arrangement;
length of service (including start date) and types of service utilized;	the type of communication service used, the technical provisions taken thereto and the period of service;
means and source of payment for such service (including any credit card or bank account number),	billing and payment information, available on the basis of the service agreement or arrangement;
local and long distance telephone connection records, or records of session times and durations;	X
Х	any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.



VOLUNTARY DISCLOSURE REQUEST/ORDER STANDARDS

1&JPN REF. 20-112

REQUEST COMPONENTS FOR ACCESS TO SUBSCRIBER INFORMATION UNDER VOLUNTARY DISCLOSURE REGIME²³

This document further develops the minimum basic components of requests formats, originally identified in the Operational Approaches,²⁴ from the perspective of access to cross-border subscriber data from public authorities to internet intermediaries.

These components do not include a provision for emergency situations including threats to life, as providers can open a separate communication channel for dealing with emergency requests. These components however allow for the indication of an expedited request to account for circumstances where a requester may be under a specific deadline.

Some components can be mandatory (i.e. a necessary condition for consideration - not necessarily sufficient for acceptance and execution, though). They are indicated with an *.

CLUSTER	LABEL	DESCRIPTION	
	Request Number*	Request ID number that identifies the specific request; used for reference tracking and potential audits.	
	Time & Date*	Timestamp on transmission from the requesting country.	
prespension	Requesting Country*	Indicates the requesting country.	
REFERENCING	Recipient Company*	Indicates the destination of the request, in particular a Point of Entry (POE).	
	Case Number	Identifies the corresponding legal case in the requesting country.	
	Previous Request Numbers	Request ID number(s) pertaining to related request(s) that have been made previously, if any.	
	Account information*	Identifies the specific target of the request: specific IP address, domain name, URL, user identifiers or accounts (specificity criteria).	
DATA SOUGHT	Data requested*	The specific user data being requested, with the highest degree of precision.	
	Time Range/Period	The time range/period for which subscriber data is sought. This can be used in case of situations where accounts have belonged to more than one person/user over time.	

^{23.} A compilation of definitions for Subscriber Information may be found in the Annex of "Cross-Border Requests for Voluntary Disclosure of Subscriber Information".

INTERNET & JURISDICTION POLICY NETWORK

^{24.} https://www.internetjurisdiction.net/uploads/pdfs/Papers/Data-Jurisdiction-Program-Operational-Approaches.pdf

	Offense	Description of the alleged offense and penalty associated with the alleged offense.
	Legal Basis*	National legal framework upon which this request 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 request.
CASE ²⁵	Summary of the Alleged Offense*	Facts, relation with the data, purpose and necessity, and when applicable charges pressed/list of offenses.
	Necessity and Proportionality*	The reasoning for requesting the above elements, taking into consideration the balance between the need to obtain the data and protection of user rights.
	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,).
EXPEDITED	Expedited Treatment	Request for expedited treatment.
TREATMENT	Rationale	Justification for expedited treatment.
	Confidentiality	Specifies whether specific circumstances justify that some parts or all of the request not be communicated to the concerned user.
CONFIDENTIALITY	Rationale for Confidentiality	Justification of non-notification.
	Confidentiality Timeline	Duration of the confidentiality exception.
AUTHODITIES	Transmitting Authority*	The authority and/or POC that has transmitted the request and its details.
AUTHORITIES	Investigating / Prosecuting Authority	Details of the authority investigating or prosecuting the case in the requesting country.
	Response Notification	Contact details in the requesting country to which response notifications should be directed to.
CONTACTS	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.
SELF-CERTIFICATION	Certification*	Self-certification by the investigating/prosecuting authority regarding the accuracy of the facts and the compliance with national procedures.
AUTHENTICITY REQUIREMENTS	Signature or official stamp	Identifies the signature and/or stamp of the transmitting authority.

^{25.} While most Labels are mandatory, Authorities will have to strike a balance with regards to the level of detail provided under each mandatory component.

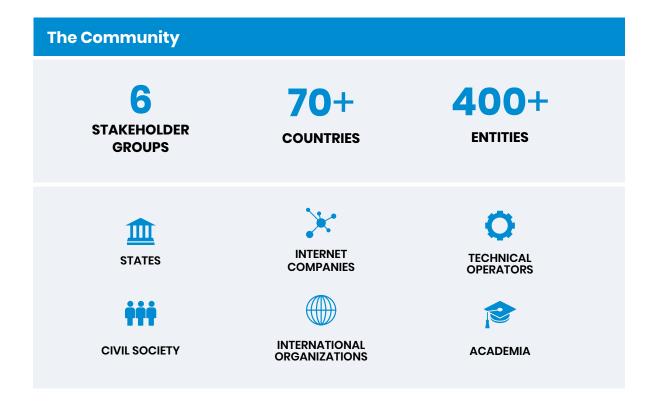
4. INTERNET & JURISDICTION POLICY NETWORK

Managing the way that a large number of separate legal frameworks apply to the internet is one of the biggest policy challenges of our time – more complex than building the internet itself.

Vint Cerf Co-inventor of the internet, writing in the Financial Times ahead of the 2nd Global Conference of the Internet & Jurisdiction Policy Network in 2018

The Internet & Jurisdiction Policy Network is the multistakeholder organization fostering legal interoperability in cyberspace. Its stakeholders 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 400 key entities from six stakeholder groups around the world including: governments, the world's largest internet companies, the technical community, civil society groups, leading universities and international organizations.

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. Host partner countries include France (2016), Canada (2018) and Germany (2019).



Mission



INFORM

The debates to enable evidence-based policy innovation

Informational asymmetry and mistrust between actors often result in uncoordinated policy action.

The I&JPN facilitates **pragmatic** and well-informed policy-making by framing issues and taking into account the **diversity of perspectives** while documenting tensions and efforts to address problems.



CONNECT

Stakeholders to build trust and coordination Cooperation is important in a digital environment that is increasingly polarized, and where actors function in policy silos, with insufficient factual information.

The I&JPN serves as the **connective tissue** between stakeholder groups, regions, and policy sectors, as well as by **bridging gaps** within governments or organizations.



ADVANCE

Solutions to move towards legal interoperability

The Policy Network strives to develop shared cooperation frameworks and policy standards that are as transnational as the internet itself. The Network promotes a balanced and scalable approach to policymaking, aiming for legal interoperability, taking inspiration from the fundamental principle that enabled the success of the internet and the World Wide Web.

Core activities



POLICY PROGRAMS



EVENTS



KNOWLEDGE MUTUALIZATION

5. ACKNOWLEDGEMENTS

This Toolkit is based on the work of the Members of the Data & Jurisdiction Program Contact Group of the Internet & Jurisdiction Policy Network 2017-2020, and its Outcome Documents, as well as the Roadmaps that resulted from the Global Conferences of the Internet & Jurisdiction Policy Network in 2016 (France), 2018 (Canada) and 2019 (Germany).

The Secretariat is grateful for the hundreds of hours of intense work of the Members of the Data & Jurisdiction Program Contact Groups, and their alternates, composed of senior level representatives from governments, internet companies, technical operators, civil society, leading universities, and international organizations from around the world since 2017.²⁶ The Secretariat also expresses thanks to Robert Young, Legal Counsel, Canada, Department of Global Affairs who serves as Contact Group Coordinator (2017–present). The following list of Members and their appointed alternates indicates the affiliation of stakeholders at the time they served in the Contact Group. Members served in their personal capacity.

Sunil Abraham, Executive Director, Centre for Internet and Society • Waiswa Abudu Sallam, Head Legal Affairs, Uganda, Communications Commission • Alejandro Amendolara, Legal Commission, Camara Argentina de Internet (CABASE) • Karen Audcent, Senior Counsel and Team Leader, Canada, Ministry of Justice • Kevin Bankston, Director, Open Technology Institute • Kerry-Ann Barrett, Cyber Security Policy Specialist, Organization of American States (OAS) • Cathrin Bauer-Bulst, Deputy Head of Unit, Fight Against Cybercrime, European Commission - DG HOME • Eduardo Bertoni, Director, Argentina, National Access to Public Information Agency • Melissa Blagitz, Federal Prosecutor, Brazil, Federal Prosecutor's Office of the State of São Paulo • Diego Canabarro, Policy Advisor, Brazilian Internet Steering Committee (CGI.br) • Joseph Cannataci, Special Rapporteur on the Right to Privacy, United Nations • Lina Cepeda, ICT Coordinator - Legal Officer, United Nations Counter-Terrorism Committee Executive Directorate (UNCTED) • Aaron Cooper, Senior Counsel, Computer Crime and Intellectual Property Section, United States, Department of Justice • Arsenio Cuenca Navarate, Trainee, Digital Research Unit, Gendarmerie • Jennifer Daskal, Associate Professor, American University Washington College of Law • Fernanda Domingos, Federal Prosecutor, Brazil, Federal Prosecutor's Office of the State of São Paulo • Brendan Eiffe, Head, Central Authority for Mutual Legal Assistance, Department of Justice and Equality, Ireland • Andrea Fabra, Public Affairs Manager, Telefonica • Camille Fischer, Frank Stanton Fellow, Electronic Frontier Foundation (EFF) • Thomas Fitschen, Director, Cyber Foreign Policy and Cyber Security, Germany, Federal Foreign Office • Sharon Bradford Franklin, Policy Director, New America Foundation's Open Technology Institute • Eric Freyssinet, Chief Digital Strategy Officer, France, Ministry of Interior • Tonia Gillett, Counsel, Office of Legal Affairs, Interpol • Hartmut Glaser, Executive Secretary, Brazilian Internet Steering Committee (CGI.br) • Robyn Greene, Privacy Policy Manager, Law Enforcement Access and Data Protection, Facebook • Nicole Gregory, Head, Data and Online Harms Policy, United Kingdom, Foreign and Commonwealth Office • Mohamed Hegazy, Head of Legislative Committee, Ministry of Communications and Information Technology • Jane Horvath, Senior Director, Global Privacy, Apple • Erick Iriarte, Coordinator of the Working Group on the Regulatory Framework of the eLAC2020 Digital Agenda, Alfa-Redi • Zahid Jamil, Barrister-at-Law, Jamil • Wookyung Jung, Cybercrime Policy Analyst, INTERPOL • Lanah Kammourieh Donnelly, Public Policy Manager, Google • 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 • Gail Kent, Global Public Policy Manager, Facebook • Monika Kopcheva, Political Administrator, Council of the European Union, Directorate-General Justice and Home Affairs • Markko Künnapu, Legal Advisor, Estonia, Ministry of Justice • Klaus Landefeld, Vice Chairman of the Management Board, Director Infrastructure & Network, Association of the Internet Industry (eco.de) • Mark Lange, Director, EU Institutional Relations, Microsoft • Emmanuelle Legrand, Legal and Policy Officer, European Commission, DG JUST • Arianna Lepore, Programme Officer, Terrorism Prevention, United Nations Office on Drugs and Crime - UNODC • Karl Linderborg, Deputy Assistant Police Commissioner, National Police Board - Finland • Tara M. Storey, Principal

26. An overview of the Members of the Content & Jurisdiction Program Group by year can be found here: https://www.internetjurisdiction.net/news/data-jurisdiction-program-contact-group-members

Officer, Irish Central Authority for Mutual Legal Assistance, Ireland, Department of Justice and Equality • Sara Marcolla, Specialist, EC3 Internet Governance, Europol • Brad Marden, Assistant Director Digital Crime Investigative Support, INTERPOL • Etienne Maury, Legal and Policy Officer, European and International Affairs Department, Commission Nationale Informatique et Libertes • Lim May-Ann, Managing Director, TRPC, and Executive Director, Asia Cloud Computing Organization • Toma Milleskaite, TBD, TBD • Drew Mitnick, Policy Counsel, Access Now • Vivek Narayanadas, Associate General Counsel, Privacy & Data Protection Officer, Shopify • Greg Nojeim, Senior Counsel and Director, Freedom, Security and Technology Project, Center for Democracy & Technology (CDT) • Takayuki Oku, Assistant Director, Cyber Strategy and Capability Development, Cybercrime Directorate, EDPS, INTERPOL • Barrack Otieno, Associate, Kenya ICT Action Network (KICTANET) • Aled Owen, Head of International Data Access, United Kingdom - Office for Security and Counter Terrorism Home Office • Han Soal Park, Lead Private Sector Outreach, Crime Prevention and Criminal Justice Officer, United Nations Office on Drugs and Crime - UNODC • Isadora Perez Peixoto, Technical Advisor, Brazilian Internet Steering Committee (CGI.br) • Erik Planken, Senior Policy Advisor Cybercrime, Law Enforcement Department, The Netherlands, Ministry of Security and Justice • Marc Porret, Senior Legal Officer, United Nations Counter-Terrorism Committee Executive Directorate (UNCTED) • Jeff Ratner, Senior Manager, Global Cybersecurity and Privacy Law, Apple • Katitza Rodriguez, International Rights Director, Electronic Frontier Foundation (EFF) • Alberto Rodriguez Alvarez, Advisor to the National Digital Strategy, Mexico, Office of the President • Vinicius Santos, Technical Advisor, Brazilian Internet Steering Committee (CGI.br) • Shamaila Sarwar, Head of Engagement, Investigatory Powers Unit, National Security Directorate, United Kingdom, Office for Security and Counter Terrorism Home Office • Acadia Senese, Law Enforcement and Information Security Counsel, Google • Bernard Shen, Assistant General Counsel, Microsoft • Christoph Steck, Director, Public Policy and Internet, Telefonica • Adil Sulieman, Senior Policy Officer, African Union Commission • Dan Suter, Director, IJust • Dan Svantesson, Professor, Bond University • Peter Swire, Professor, Georgia Institute of Technology, Scheller College of Business • Paloma Villa-Mateos, Public Policy Manager, Telefónica • Andrew Warnes, Assistant Secretary, National Security Policy Branch, Australia, Department of Home Affairs • Nathan Whiteman, Assistant Director, Australia - Department of Home Affairs • Chris Wilson, Senior Manager, Public Policy (Internet Governance), Amazon Web Services • Herbert Gustav Yankson, Chief Superintendent of Police, Ghana, Police Service • Moctar Yedaly, Head, Information Society Division, African Union Commission

I&JPN SECRETARIAT

LEAD DATA & JURISDICTION PROGRAM:

Bertrand de la Chapelle, Executive Director
Ajith Francis, Policy Programs Manager
Han Soal Park, Director Data & Jurisdiction Program
(September 2019–September 2020)
Sophie Tomlinson, Communications and Outreach Manager
Juri Wiedemann, Young Professional

Paul Fehlinger, Deputy Executive Director

Martin Hullin, Director of Operations and Knowledge Partnerships

Hedvig Nahon, Events and Office Manager

FINANCIAL AND INSTITUTIONAL SUPPORTERS

This Toolkit would not exist without the support of the unique coalition of governments, international organizations, businesses, technical operators and foundations, which enable the work of the Internet & Jurisdiction Policy Network.

Please consult the overview of these key actors and their logos at <u>www.internetjurisdiction.net/about/funding</u> The Internet & Jurisdiction Policy Network is the multistakeholder organization fostering legal interoperability in cyberspace. Its stakeholders 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 400 key entities from six stakeholder groups around the world including: governments, the world's largest internet companies, the technical community, civil society groups, leading universities and international organizations.