

**INTERNET
& JURISDICTION**

A GLOBAL MULTISTAKEHOLDER
POLICY NETWORK

DATA & JURISDICTION PROGRAM:

CROSS-BORDER ACCESS TO USER DATA

Problem Framing
May 2017



ABOUT INTERNET & JURISDICTION

Internet & Jurisdiction is the global multistakeholder policy network addressing the tension between the cross-border Internet and national jurisdictions. It facilitates a global policy process to enable transnational cooperation and preserve the global character of the Internet. Founded in 2012, the policy network engages key entities from different stakeholder groups around the world.

Internet & Jurisdiction helps catalyze the development of shared cooperation frameworks and policy standards that are as transnational as the Internet itself in order to promote legal interoperability and establish due process across borders.

© 2017 by Internet & Jurisdiction

This work is licensed under a creative commons attribution – non-commercial – no derivatives license.
To view this license, visit www.creativecommons.org.
For re-use or distribution, please include this copyright notice.



INTERNET
& JURISDICTION

14 rue Alexandre Parodi
75010 Paris, France
www.internetjurisdiction.net

DATA & JURISDICTION

After five years of exchanges in the Internet & Jurisdiction policy network, three concrete issue areas were collectively identified as priority fields for action: cross-border requests for access to user data, content takedowns, and domain suspensions. Transnational due process mechanisms are necessary in each case. In early 2016, Internet & Jurisdiction launched its first series of thematic programs to better hone, structure, and support the corresponding activities of the I&J process. Based on the 2016 Global Internet and Jurisdiction Conference, this document presents a general framing of the DATA & JURISDICTION program.



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

Criminal investigations increasingly require access to information about users and digital evidence stored by private companies in jurisdictions outside the requesting country. Existing systems for cross-border user data requests are under stress and the problem is compounded by the difficulties of determining location and jurisdictional nexus in investigations. What are the necessary safeguards and procedures to establish viable and scalable frameworks?

A TRANSBORDER CHALLENGE

Within each country, law enforcement investigations are conducted according to strict national procedures for access to and use of user data. To avoid abusive access, different national safeguards exist to reconcile the protection of citizens' rights and privacy, with the necessary restrictions thereof to address illegal activities. The digitization of societies and the increasing volume of cross-border data flows however directly impact this traditional legal landscape, introducing a strong transborder dimension:

- Instead of physical documents or objects, criminal evidence is increasingly in the form of digital data regarding the identity of internet users and their activity online.
- Potential evidence is collected and stored by a broad diversity of private companies (most large ones being based in the US) rather than located in the physical property of the investigated person.
- The amount and diversity of the collected data is growing exponentially, even in the absence of data retention obligations and especially since the development of mobile apps.
- Access to digital evidence is important not only for online crime but also for most, if not all, investigations regarding illegal activities in the physical space.
- Private companies are very often incorporated or store their information outside of the country conducting the investigation. The connection nexus of the investigated crime with a foreign country can be limited to the use of such services.
- The development of cloud services makes the actual location of data more uncertain, while the lack of working solutions can increase calls for data localization.
- The large-scale deployment of end-to-end encryption makes it more difficult for national authorities to access certain data, which increases tensions.

In light of this increasingly transnational dimension of investigations, there are two main mechanisms presently employed for cross-border access to user data present significant limitations.

TWO APPROACHES

MLATs. International legal cooperation is traditionally handled through Mutual Legal Assistance Treaties (MLATs). However, this was initially designed to handle relatively rare cases and the MLAT system therefore struggles to adapt to the massive evolutions described above. Generally regarded as slow and complex, it needs reform and some efforts are under way in that regard. Yet, even an improved MLAT system is hardly scalable to all countries, and moreover imposes the law of the recipient country even when the case at hand has no connection to it. Frustration with this system encourages states to use national production orders based on the mere provision of services to users in their country, or impose compulsory data localization requirements, both of which present challenges of their own if they were generalized around the world.

Direct requests to intermediaries. In that context, requests for access to user data are increasingly sent directly by law enforcement in one country to internet intermediaries in another to solicit voluntary cooperation. The number of such requests increased by 40% between 2014 and 2015¹. In the United States, the Electronic Communications Privacy Act (ECPA) allows voluntary communication of basic subscriber identification (BSI) and traffic data by private companies to foreign law enforcement. Most companies mention their right to do so in their Terms of Service. So-called content data, however, still needs to be obtained through MLAT in application of the Stored Communications Act (SCA). Determining the validity of a request therefore becomes the responsibility of private entities, increasingly tasked with evaluating the applicability of a patchwork of national laws and procedures without a clear and transparent reference framework. Moreover, conflicting legislations regarding conditions for voluntary transborder cooperation can place companies in a dilemma when complying with the law of one country implies breaking the law in another.

All stakeholders face the common challenge of reconciling several competing objectives. Their joint responsibility could be described as: **Developing policy standards respecting privacy and due process and defining the conditions under which authorized law enforcement authorities can request from foreign entities access to stored user data necessary for lawful investigations.**

¹ From parties to the Budapest Convention (excluding the United States) to 6 key US-based operators. Source: Council of Europe's Cloud Evidence Group Report.

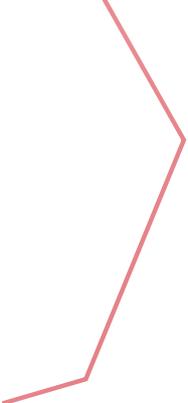
CURRENT INITIATIVES

Tensions regarding cross-border access to data are increasing in different regions around the world. Specific discussions are under way in the United States and Europe to improve cross-border access to user data through voluntary cooperation, with significantly different yet potentially complementary approaches emerging in regard to access to content and non-content user data:

European Union. On March 7-8, 2016, the Dutch Presidency of the European Union convened the “Crossing Borders: Jurisdiction in Cyberspace” conference in Amsterdam. Participants explored these issues in detail and highlighted the importance of access to basic subscriber information. The conference conclusions fed into the meeting of the European Council of Ministers for Justice and Home Affairs on June 9-10, 2016. The resulting Conclusions of the Council tasked the European Commission to “develop a common framework for cooperation with service providers for the purpose of obtaining specific categories of data, in particular subscriber data” which would set “commonly agreed requirements.” The Commission was also tasked with engaging service providers “to explore [...] the possibility of using aligned forms and tools” such as “a secure online portal for electronic requests and responses.”

Council of Europe. Home of the 2001 Convention on Cybercrime, the Council of Europe has devoted significant efforts to this issue within its T-CY Committee, in particular its Cloud Evidence Group, which issued its report in September 2016. Various approaches were suggested in the report, including: “practical measures to facilitate transborder cooperation between service providers and criminal justice authorities”; the production of a Guidance note on Article 18 of the Budapest Convention to clarify, inter alia, when a provider is “offering services in the territory” of the requester; and even the possible development of an additional protocol to this treaty. The Guidance Note on Article 18 was published in early 2017.

CDBR Working Group. Since the end of 2015, a possible regime for cross-border access to so-called “user content data” (not only basic subscriber information or traffic data) has been explored by an informal group of US-based actors from academia, civil society, and key internet platforms, with the US government (including the Department of Justice) as observer. This regime would apply when the



only nexus of connection with the US is the use of a US-based service provider, i.e. if the “requesting government has jurisdiction over both the target and the relevant criminal activity.” The target should not be a US citizen or located in the United States. In such cases, an exception to the Electronic Communications Privacy Act (ECPA) and Stored Communications Act (SCA) would allow companies to voluntarily disclose user content data to foreign law enforcement, under specific and predefined procedural guarantees and safeguards.

US-UK Draft Agreement. Discussions were initiated in 2016 regarding a US-UK bilateral agreement for reciprocal cross-border access to data. It would allow law enforcement and security authorities with lawful local warrants to obtain data directly from communication services providers in the other country more quickly and simply than through MLATs. Similar bilateral agreements could be progressively established with other countries. A proposed bill has been tabled in the US Congress to enable this mechanism. However, these discussions may be impacted by recent divergent court decisions. The US Second Circuit Court of Appeals in January 2017 upheld that US authorities cannot directly request data stored in Microsoft’s Irish servers. But the District Court for the Eastern District of Pennsylvania in February 2017 ruled in the opposite direction (about Google), as did the Eastern District of Wisconsin (February 2017) and the Middle District of Florida (April 2017). This divergence makes the capacity of US authorities to access data stored overseas by US companies uncertain, and could constrain such bilateral negotiations, unless the issue is directly addressed by Congress.

Consultations between these different initiatives are necessary to ensure policy coherence, as well as the involvement of the different stakeholders. Furthermore, early engagement of actors beyond Europe and the US is required to foster scalability.



AREAS OF COOPERATION

The first Global Internet and Jurisdiction Conference, held in Paris on November 14-16, 2016, gathered more than 200 senior representatives from the different stakeholder groups in the I&J Policy Network. Exchanges conducted there and in the following months on this issue helped identify a limited list of "areas of cooperation" and the following concrete questions to structure further discussions.

1. TRANSPARENCY

- 1.1 How can the clarity and comparability of transparency reports be further strengthened? How could governments also produce similar information?
- 1.2 When and under which conditions can and should users not be notified of requests for their data?

2. JURISDICTIONAL CRITERIA

- 2.1. What criteria (territorial or otherwise) should determine the right to request access to user data — location of company, data centers, users, victims, crime, or a combination thereof?
- 2.2. How can the geographic scalability of the proposed approaches be ensured?

3. REQUEST PROCEDURES

- 3.1. What core elements should a proper request for user data contain, and which corresponding standards should it meet?
- 3.2. How can requests be authenticated? How could a database or registry of single points of contact be created?
- 3.3. How different should procedures be for access to basic subscriber information, traffic data, and content data?

4. DUE PROCESS STANDARDS

- 4.1. How should standards be determined?
- 4.2. How can proper appeal and redress mechanisms be developed across borders?

RESOURCES

KEY BACKGROUND DOCUMENTS

US-UK BILATERAL AGREEMENT

US Department of Justice Testimony at a Congressional Hearing (February 2017)

<https://judiciary.house.gov/wp-content/uploads/2016/02/doj-bitkower-testimony.pdf>

White Paper prepared for US Congress (March 2016)

<http://www.netcaucus.org/wp-content/uploads/20160310-US-UK-Hill-Leave-Behind-Final.pdf>

Draft legislation proposed to US Congress (July 2016)

<http://www.netcaucus.org/wp-content/uploads/2016-7-15-US-UK-Legislative-Proposal-to-Hill.pdf>

CBDR WORKING GROUP (“DASKAL-WOODS” PROPOSAL)

Initial post by Jennifer Daskal and Andrew Woods (November 2015)

<https://lawfareblog.com/cross-border-data-requests-proposed-framework>

Article by Jennifer Daskal (2016)

<http://jnslp.com/wp-content/uploads/2016/09/Law-Enforcement-Access-to-Data-Across-Borders.pdf>

EUROPEAN UNION

Discussion paper on tackling cybercrime (January 2016)

<https://english.eu2016.nl/documents/publications/2016/03/7/general-discussion-paper-justice-ministers-meeting-cybercrime>

Conference: "Crossing Borders: Jurisdiction in Cyberspace" (March 2016)

<https://english.eu2016.nl/events/2016/03/07/crossing-borders-jurisdiction-in-cyberspace>

Conclusions of the Council of Ministers of Justice and Home Affairs (June 2016)

http://www.consilium.europa.eu/en/meetings/jha/2016/06/Cyberspace-EN_pdf/

COUNCIL OF EUROPE

T-CY Committee

<https://www.coe.int/en/web/cybercrime/tcy>

Cloud Evidence Group

<https://www.coe.int/en/web/cybercrime/ceg>

T-CY Paper: “Criminal Justice Access to Electronic Evidence...” (February 2016)

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805a53c8>

Final report of the Cloud Evidence Group to the T-CY (September 2016)

<https://www.coe.int/en/web/cybercrime/tcy>

T-CY’s Guidance Note on Art. 18 of the Budapest Convention (March 2017)

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806f943e>

INFLUENTIAL COURT DECISIONS

UNITED STATES: Concerning the reach of search warrants on data stored abroad
Microsoft wins landmark appeal over seizure of emails stored in Irish jurisdiction (2016)

http://www.internetjurisdiction.net/publications/retrospect#article-5542_2016-07

Pennsylvania district court says Google must comply with domestic warrants for data stored abroad (2017)

http://www.internetjurisdiction.net/publications/retrospect#article-5605_2017-02

Eastern District of Wisconsin ruling on domestic warrants for data stored abroad (2017)

<http://www.netcaucus.org/wp-content/uploads/2016-7-15-US-UK-Legislative-Proposal-to-Hill.pdf>

Florida Middle District Court rejects the Second Circuit decision (April 2017)

<https://www.justsecurity.org/wp-content/uploads/2017/04/Florida-case.pdf>

BRAZIL: WhatsApp blocked in Brazil for failing to comply with user data request (2016)

http://www.internetjurisdiction.net/publications/retrospect#article-5543_2016-07

INDIA: Court orders YouTube to share user data related to a defamation case (2016)

http://www.internetjurisdiction.net/publications/retrospect#article-4079_2016-10

BELGIUM: Government refuses MLAT procedure, asserts jurisdiction over Yahoo (2015)

http://www.internetjurisdiction.net/publications/retrospect#article-5407_2015-12

SELECTION OF RELATED CONTRIBUTIONS

COMMENTS ON ACCESS TO USER DATA

Albert Gidari (Stanford Center for Internet and Society)

<https://cyberlaw.stanford.edu/blog/2016/02/mlat-reform-and-80-solution-whats-good-users>

Mark Jaycox and Lee Tien (Electronic Frontier Foundation)

<https://www.eff.org/deeplinks/2015/12/reforms-abound-cross-border-data-requests>

Greg Nojeim (Center for Democracy & Technology)

<https://cdt.org/files/2016/08/DOJ-Cross-Border-Bill-Insight-FINAL2.pdf>

Jennifer Daskal (American University)

<https://www.justsecurity.org/39959/microsoft-ireland-fix-time-act-now/>

COMMENTS ABOUT THE US-UK NEGOTIATIONS

Andrew Woods (University of Kentucky)

<https://lawfareblog.com/us-uk-data-deal>

Kevin Bankston (Open Technology Institute)

<https://www.newamerica.org/oti/press-releases/oti-condemns-plan-let-uk-government-use-american-companies-internet-wiretapping/>

Vipul Kharbanda and Elonnai Hickok (Centre for Internet and Society – India)

<http://cis-india.org/internet-governance/blog/mlats-and-the-proposed-amendments-to-the-us-electronic-communications-privacy-act>

COMMENTS ON SINGLE POINT OF CONTACT (SPOCs) FOR MLAT REQUESTS

Peter Swire and Deven Desai (Georgia Institute of Technology)

<https://www.lawfareblog.com/qualified-spoc-approach-india-and-mutual-legal-assistance>

COMPANIES' TRANSPARENCY REPORTS, POLICIES, AND PORTALS

APPLE

Transparency reports

<https://www.apple.com/privacy/transparency-reports/>

Guidelines for information requests

<https://www.apple.com/privacy/government-information-requests/>

Privacy Policy

<https://www.apple.com/legal/privacy/en-ww/>

FACEBOOK

Transparency Reports (government requests)

<https://govtrequests.facebook.com/>

Guidelines for Law Enforcement

<https://www.facebook.com/safety/groups/law/guidelines>

Law Enforcement Online Request System

<http://www.facebook.com/records>

Data Policy (see “How do we respond to legal requests or prevent harm?”)

<https://www.facebook.com/about/privacy/other#>

GOOGLE (various services, including Gmail, YouTube, and Blogger)

Transparency report section on user data requests

<https://www.google.com/transparencyreport/userdatarequests/?hl=en>

Legal process for handling requests for user information from outside the US

https://www.google.com/transparencyreport/userdatarequests/legalprocess/#how_does_google_respond

Privacy Policy (see “Compliance and cooperation with regulatory authorities”)

<https://www.google.com/policies/privacy/#enforcement>

MICROSOFT

Transparency Report (law enforcement requests)

<https://www.microsoft.com/about/csr/transparencyhub/ler/>

Principles, Policies and Practices FAQ

<https://www.microsoft.com/about/csr/transparencyhub/pppfaq/>

Privacy Statement (see “Reasons We Share Personal Data”)

<https://privacy.microsoft.com/en-us/privacystatement>

TWITTER

Transparency Report (section on information requests)

<https://transparency.twitter.com/>

Guidelines for Law Enforcement

<https://support.twitter.com/articles/41949>

Law Enforcement Online Request System

<https://support.twitter.com/forms/lawenforcement>

Privacy Policy (see “Law and Harm”)

<https://twitter.com/privacy?lang=en>