CROSS-BORDER REQUESTS FOR VOLUNTARY DISCLOSURE OF SUBSCRIBER INFORMATION

INTERNET & JURISDICTION POLICY NETWORK

REF: 21-102 | March 12, 2021

Subscriber information[1] 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 procedures[2] 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 jurisdictions[3], and the type of services the provider offers.

The Internet & Jurisdiction Policy Network has previously documented[4] 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 documents[5] 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).

---

[1] 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.

[2] These procedures may naturally vary from state to state.

[3] 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.

[4] https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-20-111-General-Regime-Architecture.pdf

[5] Link to the other elements of the toolkit : 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 stored[6] by a foreign service provider incorporated in a country that does not prohibit voluntary disclosure of such information.

- *Types of Crimes covered*[7]
  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

[6] This document does not address real-time interception of electronic communications.

[7] This document does not cover emergency situations. The Contact Group may address this topic in the future.

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.

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.[8]

- *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[9], 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[10]. 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

[8] Service providers can consult human rights groups and human rights reports to identify those countries.

[9] Some Members of the Contact Group express that such requests for secrecy should be approved by a judicial or other independent oversight mechanism.

[10] National laws may prescribe such notification at different times, including when the data subject is under investigation, indicted or put on trial.

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.

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.

COMPARATIVE SUMMARY OF DEFINITIONS :

United States	Council of Europe
18 U.S.C. § 2703	*Budapest Convention* *2nd 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
X	any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.