ACCESS TO USER DATA IN THE CONTEXT OF COVID-19

REF: 20-103 | April 15, 2020

Numerous private digital services and applications routinely collect data from their users. Some of this data can be useful to public authorities fighting the current COVID-19 pandemic, in relation to its various successive stages. **Many governments are thus currently devising ways to access user data or procuring dedicated applications to collect additional information**.

Reconciling the different objectives of public health and safety, economic stability and resilience, and protection of civil liberties and personal data is a common challenge for all actors. Measures adopted under the pressure of urgency risk being imprecisely targeted, insufficiently coordinated, inefficient and even contradictory. Furthermore, they may have potentially undesirable long-lasting effects if maintained once the situation normalizes.

The Internet & Jurisdiction Policy Network[1] and its three Programs[2] have for more than five years facilitated discussions among public, private and civil society actors on jurisdictional challenges on the internet, in particular regarding access to user data by public authorities. This extensive experience has demonstrated the importance of a **common frame of reference** to properly address an issue, design solutions and evaluate their impact.

In that spirit, this Framing Brief from the I&JPN Secretariat, building on interactions with Policy Network members, presents a **list of criteria** regarding new initiatives, taken or contemplated, implying access to user data in the context of the COVID-19 crisis. It aims to assist the various stakeholders in analyzing them in this exceptional context and contribute to the design of the most appropriate solutions.

It is **structured around four major themes**: initiator(s) and beneficiaries of the initiative, purposes of the new data sharing, types of data at issue and modalities of collection, and corresponding protections.

We hope that this list will help trigger meaningful discussions on a shared basis.

Sharing of identified initiatives with the I&JPN Secretariat is strongly encouraged. Please send relevant information to: [secretariat{at}internetjurisdiction.net] with this reference in the subject line: #20-103.

[1] https://www.internetjurisdiction.net/

[2] https://www.internetjurisdiction.net/work

CRITERIA

I. INITIATION AND BENEFICIARIES

- **Initiating Authority:** national government, sub-national levels (e.g. in federal states)?
- **Legal measures:** are exceptional ad hoc legislations adopted to enable data sharing or do existing legal frameworks allow it because of emergency provisions?
- **Transnational dimension:** is there access to data across borders or only at national level?
- **Requesting/Recipient authority:** who can request/receive this data: health or security authorities?

II. PURPOSES OF THE DATA SHARING

- **Types of uses (not exhaustive):**
  - Movement mapping,
  - Contact tracing,
  - Quarantine monitoring,
  - Lockdown compliance,
  - Allocation of hospital resources and equipment,
  - Alerts (e.g. encouragement to be tested, information dissemination, notices on disinformation or misinformation)
  - Other data analysis with a nexus to the COVID-19 situation
- **Primary beneficiary:** individuals (e.g. Alerts), public authorities (e.g. Monitoring), or both (e.g. Contact tracing)

III. TYPES OF DATA AND MODALITIES OF COLLECTION

- **Types of data:** geo location of user, physical proximity between users, health information, other?
- **Sources:** infrastructure providers (telecom companies, ISPs, wifi spots), general apps, crisis specific apps, data aggregators?
- **Regularly collected data or specific apps:** is the data already collected on an ongoing basis by operators or service providers for other purposes or produced by specific apps?
- **Voluntary nature (specific apps):** is the installation of the specific app mandatory or voluntary for the user?
- **Degree of aggregation/granularity of the data?**
- **Degree of anonymization:** anonymized data, pseudonymized data, full identification?
- **Stored or real-time data?**
- **Temporality:**
  - How far back in time is stored data accessed (given data retention rules)?
  - How long is the collected data preserved?
  - Is there a delay before transmission, in particular for real-time data?
- **Frequency:** is transmission recurrent or on a request-by-request basis?

IV. PROTECTIONS

- **Consent:** degree and specificity of users' consent or knowledge regarding the collection, sharing and processing of their data?
- **Duration**: is the access limited to the period of emergency?
- **Transparency:** what level of transparency is required from states and private actors?
- **Oversight:** is it exercised by existing or ad-hoc mechanisms?
- **Restrictions to (re-)use:** in particular by security authorities beyond the health-related purposes and after the end of the emergency?
- **Confidentiality:** what requirements apply to third-party app developers and analysts outside government (e.g. academia, private research companies)?