# FRAMING BRIEF: CATEGORIES OF ELECTRONIC EVIDENCES

REF: 22/102 | May 31, 2022

For the purposes of this document, electronic evidence[1] is understood as electronic data stored by service providers that is needed for investigating and/or prosecuting criminal activity. Electronic evidence plays a critical role in not just investigating and prosecuting cybercrime, but increasingly also traditional offline crimes.

Electronic evidence contains data, which in one way or another relates to a particular individual and their personal life. Disclosure of such data can be more or less intrusive, depending on, for example, how much personal details it reveals about a targeted individual. The general principle is that the intrusion into an individual's personal life has to be proportionate to the ends for which that data is being sought.

When accessing this data, two competing interests need to be reconciled: privacy considerations (protection of an individual's personal data, especially sensitive data), and security considerations (the need to investigate and prosecute crime or ensure national security). Neither is absolute, and accessing the evidence is based upon principles of necessity and proportionality and specification of the purpose for which the evidence is gathered.

Accordingly, different categories of electronic evidence have been defined, with corresponding procedural protections[2] for obtaining it, albeit with significant disparities between countries in both regards. In particular, privacy and data protection standards differ from jurisdiction to jurisdiction. This may also be the case for what is considered sensitive data. The situation is further complicated when individuals and/or service providers reside outside the jurisdiction where the investigation is being carried out.

Definitions and standards for access to electronic evidence largely date back to the telephony or early email era, where services provided and providers were relatively homogenous, and the amount of stored data remained quite limited. However, in today's digital age, the sheer diversity of services (e.g. social media, messaging, video on demand, short form video sharing, and numerous apps) and the amount and diversity of types of data collected need to be considered. Additionally, different jurisdictions may have different definitions of service providers who will fall under legal regulations. In many cases, this definition is broad, and may actually encompass any service offered over the internet.

[1] See Authorized Public Authorities in I&JPN Cross-Border Access to Electronic Evidence Toolkit

[2] In particular, depending on the type of data requested, regarding which authorities can issue orders and whether validation by a prosecutor or a court is necessary.

This new environment puts in question the adequacy of the traditional categories and the relatively straightforward correlation between a type of data, its degree of intrusiveness, and the level of procedural protections for obtaining it.

In this context, this Framing Brief on Categories of Electronic Evidence introduces the commonly used categories of electronic evidence (Part I), then explores what trends challenge the current categorization (Part II), and proposes a new framing of the problem (Part III).

## I. THREE CLASSIC CATEGORIES OF ELECTRONIC EVIDENCE

While criminal justice standards for access to electronic evidence vary across jurisdictions, regional instruments and bilateral agreements frequently refer to three categories of electronic evidence corresponding to three levels of procedural protections, based on an ascending level of privacy intrusion for the targeted individual:

1) **Subscriber Information:** Data within this category pertains to information that can primarily be used to identify the user of a particular service. This information may be provided by the user when signing up or collected in the process of providing said service. This category often includes information such as name, address, email address, telephone numbers, etc.
2) **Traffic/Access and Transactional data:** This often includes information that may be used to ascertain the origin, duration, or date of a communication and the means of access to a particular service, as well as the links and connections with other users, including contacts. Depending on jurisdictions, this may include information pertaining to commencement and termination of the use of a service.
3) **Content data:** It concerns the content of communications and traditionally includes information such as the body of emails, text messages or photographs.

While these categories may seem clear, there can be significant spillover across them. For example, some types of traffic or access data (e.g. IP addresses) are considered to have the same protections as subscriber information. Similarly, there is an ongoing debate concerning location data and whether it falls under transactional or content data. What is in each category may also vary across jurisdictions.

These three categories directly correspond to three set thresholds of procedural and substantive protections to protect individuals' privacy and ensure due process. Concretely, subscriber information may be requested directly by law enforcement authorities, as this is usually the starting point for investigations and accessing this data is traditionally considered less intrusive than for other categories. Similarly, for Traffic/Access and Transactional data, jurisdictions often set the threshold so that orders must be issued or validated at minimum by a prosecutorial authority, while orders for content data usually require to be validated by a court.[3]

## II. THE EVOLUTION OF INTRUSIVENESS

Four interlinked evolutions make the notion of intrusiveness a critical element in the debate on access to electronic evidence:

- **An explosion of stored data:** An increasing number of human activities are conducted or reflected digitally. The resulting explosion of data is not only increasingly recorded but also kept for longer periods of time, in the interest of both providers and users. This is facilitated by the dwindling costs of storage, particularly in the cloud. Most of this data, such as the very substance of interactions in social media and messaging, would not have been accessible in the telco and early email era without intrusive actions such as wiretapping, that require much higher procedural guarantees than access to content.
- **More specialized services:** Not only has the number of services and applications exploded, but they increasingly cater to specific communities and interest groups. As a result, even basic subscriber information, which generally can be accessed by law enforcement authorities without a court order, may reveal highly sensitive information. For instance, obtaining a subscriber information request to certain dating sites may reveal a user's sexual orientation. Such information is categorized as sensitive information and justifies a higher level of protection.
- **New types of data:** The collection of detailed profiles, interests or browsing activity, smart devices monitoring and logging an individual's moves and bodily functions, or the emerging field of XR and metaverses, potentially turn into electronic evidence biometric, neural, or even behavioral data. There is a lack of clarity on how such information fits within the existing typology of traffic, access and content data, or whether they justify new classifications of their own. Likewise, increased datafication through IoT devices results in new data points previously undocumented or accessible - for example: smart meter data can help ascertain use of water or electricity at particular times at a crime scene, or wearables reveal a suspect's health and vital statistics.
- **New methods of analysis:** Given the amount and very diverse types of data collected, it is difficult to clearly pinpoint the potential of a certain type of data to inform about a user. Increased computing power and powerful algorithms can tap into the vast pool of accessible data in previously inaccessible ways and through correlations, infer sensitive conclusions. For instance, graphical representation of a series of location points, coupled with map data

[3] In addition, when Mutual Legal Assistance mechanisms are used for cross-border access, orders may have to be validated by courts in the receiving state.

can identify sites visited (e.g. an abortion clinic) and biometric information, which may be considered as subscriber information, can be recombined with other information gathered in the course of the investigation.

These trends compel a re-evaluation of the notion of intrusiveness, understood as how access to certain data may affect individuals and intrude into their private life. The level of procedural protections for accessing electronic evidence was clearly related to the perceived intrusiveness of traditional data categories. Yet, as the relation between data categories and intrusiveness becomes less clear, the existing procedures linked to the categories of data may no longer ensure adequate protections and sufficient checks and balances. This development is creating an increasingly complex process of identifying the level of intrusiveness against rigid categories.

## III. STRUCTURING THE NECESSARY DEBATE

Current regulatory frameworks are therefore being challenged, and there is no simple answer. Moving forward, the following three interdependent clusters of questions can help frame the necessary discussion:

### How to define the appropriate levels of protection?

To a large extent, traditional categories were a proxy for the level of protection corresponding types of data should receive, based on perceived level of intrusiveness. In the telecoms and early email era, when both service providers and types of data collected were limited and relatively homogenous, this binary relationship was considered enough to ensure that sensitive data be afforded adequate due process protections. But this simple nexus between type of data and intrusiveness is blurring. In particular, apparently low sensitivity data obtained for one purpose (e.g. mere user identification) may, because of the nature of the service or later recombination with other data, provide significantly more intrusive insight into a targeted person's life. Defining appropriate levels of protection becomes more complex. Some key framing questions in that regard are:

- Are the existing three levels[4] of procedural protection still sufficient, and if not, what potentially stronger protections may be applicable for such sensitive data?
- Should the setting of the appropriate levels of protection to ensure proportionality and due process result from a multi-factor analysis, beyond just the nature of the data itself?
- If so, what all should such a multi-factor analysis take into account: The nature of the service? The initial stated purpose of obtaining this data? The consequences of its potential reuse and recombination at later stages of the investigation? Sensitivity of the data? Other criteria?

[4] See part 1 above

- Can this be codified in laws or regimes in sufficiently clear detail or would a case-by-case analysis have to be conducted? If so, by whom and at what stage? And how then to ensure predictability?
- What are the rules regarding the duration of storage of such electronic evidence and its ultimate deletion?
- How should procedural protections apply when data initially acquired for a particular use (i.e. identification of a user), is potentially reused at a later stage for a different purpose, or even for investigating a new crime? Should there be a process of re-authorization for using such data apart from rules regarding admissibility in court?

### What is the future of categorization?

The current categorization is determined by applicable national laws to ensure clarity and predictability. Yet, significant variations exist across countries, and, as the landscape evolves in terms of both data collected and diversity of providers, concerns arise pertaining to whether and how new types of data can fit into existing categories. Definitions unavoidably oscillate between two extremes: not being flexible enough to adapt to changes or being too open to multiple interpretations. While standardization is welcome, it is difficult to achieve across jurisdictions, and may introduce some unnecessary rigidity. Some key framing questions are therefore:

- Should categorization remain an objective, or is the determination of applicable procedural protections sufficient?
- If so, should new categories of electronic evidence be introduced, and if so, which ones?
- How to make categorization more adaptive, avoiding both excessive rigidity and unpredictability?
- How to develop definitions of types of data that ensure cross-border interoperability, and through what process(es)?

### Should every type of digital data be requestable?

Collected and stored data now pertains to vastly more aspects of an individual's life, choices or characteristics. This includes, inter alia, extensive location, behavioral or health-related data, as well as biometric data (e.g. fingerprints, voiceprints, or even eyeball movements and pupil dilation), not to mention information from various smart assistants and IoT devices. Moreover, lasting storage of previously ephemeral information now enables potential access to what previously required highly regulated actions by law enforcement (e.g. surveillance, wiretapping). In addition, some types of data may not only reveal information about a targeted user, but also information regarding other users (eg: smart goggles or AR/VR headsets might record and monitor surroundings).

This evolution profoundly changes the nature of what criminal evidence was in the offline world (e.g. documents or physical objects of all sorts) or even in the early digital era (e.g; local computer records or generic email communications). A growing societal challenge is therefore: should every type of digital data stored by service providers, irrespective of its sensitivity and level of intrusion, be potentially accessible by law enforcement in the investigation and prosecution of a crime? Some key framing questions in that regard are:

- If every type of digital data is requestable, are the current types of due process standards sufficient? Should new procedures be developed regarding some data types or uses thereof, taking inspiration for instance from more restrictive regimes (e.g. wiretapping)?
- If not, what types of data or uses (or any combination thereof) should be considered out of bounds? And how and by whom can this be determined?

## CONCLUSION

The traditional approach of three rigid categories with corresponding lists of types of data and protections have now been enshrined in various national, international and bilateral instruments (including the 2nd Additional Protocol to the Budapest Convention on Cybercrime). This represents a clear rigidity and path of dependency on these categories in the discourse around access to electronic evidence.

However, as documented above, this approach is increasingly challenged by the volume of data generated and collected, the emergence of new services and data types, as well as the ways this data can be analyzed. The regulatory framework(s) that suited electronic evidence in the telephony and early email era struggle to handle a much more heterogeneous digital landscape, in particular when the increasingly cross-border dimension of access to electronic evidence has to be taken into account.

This creates an unavoidable tension that will only grow in the years to come. In a context of constant change, reconciling predictability and adaptability in terms of appropriate due process guarantees demands a more agile approach, which may include new types of rules and potentially the creation of new coordination structures.

In any case, this highly complex challenge requires a meaningful and constructive debate among a broad diversity of actors, if we are to reach sufficient common understanding, avoid incoherent or even conflicting approaches, and achieve the necessary interoperability.