Information on Legal Frameworks in Paraguay Pertaining to Privacy and Freedom of Expression

1. PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

1.1 Paraguayan Constitution

Article 36 of the Paraguayan Constitution provides a right to privacy of communications and freedom from interception. However, there is an exception by way of judicial order in cases specified by law and when such interception would be indispensable for clarifying matters within the competence of the relevant authorities. It also states that the law will determine the modalities of such interception and that any evidence obtained in violation of these requirements is inadmissible.

1.2 Criminal Procedure Code (Law 1286/98)

Under article 200 of the Criminal Procedure Code, judges of the Criminal Courts may, at the request of the Public Prosecutor's Office ("**PO**"), in exceptional circumstances and by reasoned order, authorise the interception of an accused's communications by any technical means deemed necessary. In accordance with Article 36 of the Constitution, in order to be 'exceptional' the interception must be indispensable for the clarification of the matter at issue. The judge has discretion to determine who should execute the interception.

The results of such an interception must be provided to the judge who authorised it. The judge must then order the destruction of any irrelevant material before any results are made available to the PO, the accused and the accused's legal counsel.

1.3 Law 1881/02

Law 1881 of 2002 sets out offences and procedures relating to narcotics and dangerous drugs. Under article 88, the National Anti-Drug Secretariat (known as "**SENAD**") or the PO may apply for judicial authorisation from the Criminal Court to intercept communications. Such an application must contain details of the types of communications to be intercepted, the technical means proposed for performance of the interception, and the objectives of the interception. The judge may also request further evidence in support of the application.

To obtain the authorisation, the applicant must show that the interception is necessary and appropriate for fulfilling its objectives. The order must explicitly identify the agents responsible for executing the interception and the duration of the authorisation.

Under article 89, the authorising judge and the PO must monitor and coordinate the interception operation as it progresses and all evidence obtained must be made available to them.

1.4 Law 5241/14 Creating the National System of Intelligence

The National Secretary for Intelligence (known as "**SINAI**") can apply to the Criminal Court of Guarantees in the area where the interception is to take place for judicial authorisation to intercept communications (article 26). Such authorisation will only be granted when the information sought cannot be obtained from public sources and is strictly necessary to fulfil the state's goals of safeguarding peace, national security and

institutional stability, protecting the people from terrorism, organised crime and drug trafficking and defending the rule of democracy (article 26).

The judge must provide a reasoned decision within 24 hours and the order must state the means to be used, the person(s) to whom the measures will apply and the duration of the authorisation. The judge can authorise interception for periods of up to 90 days but this can be renewed once for another period of up to 90 days.

In accordance with article 27, the SINAI must submit the results of the interception to the judge who ordered it. The judge must then review them to ascertain the relevant products of the interception and order the destruction of any irrelevant material.

1.5. Law 12515/1996 Creating the Ministry of the Interior

This law provides for the creation of the Intelligence Direction under the authority of the Homeland Secretary (known as "**Ministerio del Interior**") which, as one of the agencies included in SINAI, has the power to request to court orders for lawful interception of communications in order to preserve internal security in accordance with the procedures set out above.

2. DISCLOSURE OF COMMUNICATIONS DATA

2.1 CONATEL Resolution 1350/2002

Article 1 of this resolution obliges communication service providers ("**CSPs**") to retain the inbound and outbound call records of its subscribers for a maximum of six months. Under articles 89 and 90 of the Telecommunications Law 642/95, information relating to the contents and existence of such communictions cannot be disclosed except by court order.However, in its ruling N° 674/10, the Supreme Court of Justice declared that disclosure of communications metadata could be ordered not only by the court also by order of the PO. National security and emergency powers

3. NATIONAL SECURITY AND EMERGENCY POWERS

3.1 Paraguayan Constitution

Article 288 of the Constitution states that in cases of armed international conflict or grave internal unrest that put the rule of the constitution or the government agencies created under it in imminent danger, Congress or the President may declare a state of emergency.

If declared by the President, the declaration must be validated by Congress within 48 hours. The declaration can last for an initial period of up to 60 days but may be extended by periods of up to 30 days with the approval of an absolute majority in both Congress and the Executive.

Article 238 also gives the President, with Congressional approval, the power to declare a state of national defence as discussed further below.

3.2 Executive Order 14135 of July 15, 1996 regulating Law No. 642 on Telecommunications

Article 14 of this order states that if a state of emergency is declared in accordance with article 288 of the Constitution, all telecommunication service operators must prioritise the transmission of the communications of the National and Civil Defence Systems.

The National Telecommunications Commission, through the Commander in Chief of the Armed Forces, may also take direct control of telecommunications services. However, this does not give any government agency the power to disregard the right to privacy of communications provided by article 36 of the Constitution. Therefore any interception measures must still be subject to the processes and authorisation detailed above.

There is no legal right on the part of telecommunications providers to appeal or seek compensation in relation to any of these decisions.

3.3 Law 1337/97 Regarding National Defence and Internal Security

Article 16 allows the President, on declaration of a state of national defence, to deploy, integrate and mobilise all national resources for the purpose of national defence. Article 20 states that, in such a situation, the President may order the requisition of services or goods to satisfy the needs of national defence. However, this does not give any government agency the power to disregard the right to privacy of communications provided by article 36 of the Constitution. Therefore any interception measures must still be subject to the processes and authorisation detailed above.

4. CENSORSHIP-RELATED POWERS

4.1 Law of Judicial Organisation (Law 879/1981)

There are no explicit legal powers which allow any government agency to require that a CSP block access to any IP address. However, in cases of inadequacy, obscurity or silence of the law, judges have the power to apply the general principles of law. Under this framework, the Criminal Court could order CSPs to block the IP addresses connected to websites involved in the commission of a criminal offence.

5. PUBLICATION OF LAWS AND AGGREGATE DATA RELATING TO LAWFUL INTERCEPT AND COMMUNICATIONS DATA REQUESTS

5.1 Publication of laws

There are no legal restrictions in Paraguay on the publication of laws or information relating to them.

5.2 Publication of aggregate data

In accordance with article 36 of the Constitution, CSPs are prohibited from publishing any information, including aggregate data (such as volume of interception requests), in relation to the interception powers detailed above.

Furthermore, article 22 of Law 5241 states that documents, records and files relating to intelligence and counterintelligence activities must be kept confidential for a period

of up to 20 years as determined by the SINAI. Article 23 goes on to state that any institutions which become aware of such documents must keep both the existence and content of such documents confidential until they are declassified by the SINAI.

In relation to SENAD investigations, article 91 of Law 1881 states that all parties involved in covert operations must keep information relating to them strictly confidential.