CISPE.cloud

27 October, 2017

CISPE Response to the Public consultation

on improving cross-border access to electronic evidence in criminal matters

CISPE is pleased to submit this response to the public consultation on improving cross-border access to electronic evidence in criminal matters. The purpose of our response is to provide the Commission with key recommendations for the upcoming legislative process.

We recognize the legitimate needs of law enforcement authorities to investigate criminal and terrorist activity, and cooperate with them when they observe legal safeguards for conducting such investigations.

However, **upon receipt of valid and binding order of a governmental body** cloud service provider should be able to cooperate in ways that are **(i) proportionated to the threat and (ii) consistent with protecting consumer privacy, security of the network and legitimate customer's needs (iii). respect for other countries' laws**

1. Consistency with protecting consumer privacy, security of the network and legitimate customer's needs is key

1.1 Privacy, security and encryption

A legislative proposal requiring companies to undermine integrity and security of their products, infrastructure and services would be detrimental for technological innovation, privacy of customers and security of networks.

CISPE believes that recent jurisprudence [1] of the Court of Justice of the European Union ('CJEU') already provides robust safeguards protecting fundamental rights and should be taken into account. Any solutions found at EU level need to respect the rule of law and fundamental rights.

Many cloud infrastructure providers offer customers options to implement strong encryption for their customer content in transit or rest, and also provides customers with the option to manage their own encryption keys or use third party encryption mechanisms of their choice. In certain cases Cloud Service providers do not have access to the data requested by competent authorities since it is encrypted.

It is key that the consultation should not lead to a requirement for Cloud service providers to reverse engineer, provide back doors or any other technology mandates to weaken the security of its service.

As the Commission continues to debate the encryption issue, CISPE advocates for policies that set the standard for security policies that protect the privacy and freedom of citizens.

1.2 Legitimate customer's needs

Unfortunately, we are aware that customers often do not want to put their data in a cloud infrastructure outside their national borders in part due to the concern that law enforcement in another country could obtain their data. This concern is driven by a lack of clarity in the laws as to whether a user could contest the government's demand in the same way as they could before they had moved information to the cloud.

[1] Court of Justice of the EU: Case C-399/11; Case C-411/10 –concluding that even measures derogating from EU law are subject to the Charter of Fundamental Rights

Our members carefully examine each request to authenticate its accuracy and verify that it complies with applicable law. If they are compelled to disclose customer content, it is important that companies are able to notify their customers.

Any solution to improving criminal justice in cyberspace must consider the need for users of cloud based infrastructure.

2. Proportionality to the threat

We believe requests to access to data need to respect procedural safeguards and the rule of law. Accordingly, any request has to be "reasoned", based on law and subject to review and decision by a court or an independent administrative body and be limited to what is strictly necessary for the investigation in question and target individuals implicated in the crime.

Unless cloud service providers are bound by a binding court order, they will not to disclose a data request due to the fact that it could jeopardise the investigation. Companies are vigilant about protecting customers' content and they will not disclose their content unless required to do so in order to comply with a valid and binding order of a governmental body (such as court order).

When they receive a request for content from a foreign governmental body, we require that body those governments to follow long-established, internationally agreed upon processes between countries, such as through the framework of a mutual legal assistance treaty or a European Investigation Order, where applicable.

We believe that EU policy responses must consider possible reciprocal responses by third countries aiming to access data about European users. Whatever approach is adopted by the EU is likely to be replicated by others. Unilateral approaches by the EU to demand data outside Europe would only justify similar approaches by third countries to access data in Europe. As a result, the EU should adopt an approach that it would feel comfortable with other countries following.

3. Respect for other countries' laws

In developing any new EU legal framework, the Commission needs to ensure respect for other countries' laws, and by extension eliminate conflicting legal obligations – both among European Member States and with the laws of countries outside of the EU – that are placing cloud providers in an untenable position.

Queries are often raised about the rights of domestic and foreign government bodies to access content held in cloud services. Customers are often confused about issues of data sovereignty, including whether and in what circumstances governments may have access to their content.

The local laws that apply in the jurisdiction where the content is located are an important consideration for some customers. However, customers also need to consider whether laws in other jurisdictions may apply to them. Customers should seek advice to understand the application of relevant laws to their business and operations.

When concerns or questions are raised about the rights of domestic or foreign governments to seek access to content stored in the cloud, it is important to understand that relevant government bodies may have rights to issue requests for such content under laws that already apply to the customer.

For example, a company doing business in EU country (e.g. Italy) could be subject to a legal request for information even if the content is stored in another EU country (e.g. Germany). Typically, a government body seeking access to the data of an entity will address any request for information directly to that entity rather than to the cloud provider.

Cloud service providers should be able to refuse to comply when compliance would cause them to breach the law of another Member State or third country.

One way to address this would be to entitle the provider to demand that a production order be re-routed via European Investigation Order (EIO) Directive or Mutual legal Assistance (MLA) channels if it has legitimate conflict of law concerns. We support the use of EU mechanisms such as the European Investigation Order ("EIO") but more work is needed for such instruments to become viable solutions. The EIO is not binding and not all EU Members States have implemented it.

Unilateral assertions of jurisdiction by either EU member states risks potential conflicts of laws given the restrictions on data transfers or disclosures imposed on service providers by the General Data Protection Regulation and the Stored Communications Act in the US.

Additionally, the creation of a single point of contact for law enforcement/judiciary requests, which has shown real improvements in countries where it exists, is an example of how cooperation can lead to workable solutions.

Conclusion

We trust that CISPE suggestions will be taken into consideration to ensure a proportionate approach to law enforcement cross-border access to eEvidence. CISPE stands ready to constructively engage with all stakeholders involved in this crucial piece of EU legislation.

***