DIGITALEUROPE

The Software Alliance

BSA

Computer & Communications Industry Association
Tech Advocacy Since 1972

Brussels, 8 December 2016

EU Justice and Home Affairs Council
Council of the European Union
175 Rue de la Loi
B-1048 Brussels

RE: **Improving criminal justice in cyberspace; cooperation with online service providers**

Dear Ministers,

We, the undersigned associations, are writing to you ahead of your discussion on improving law enforcement access to data and the role of communications service providers in criminal investigations during the next Justice and Home Affairs Council meeting, on December 9.

We endorse greater cooperation between service providers and Member States' law enforcement authorities. Our member companies are responsible providers of hardware, software and services that work with law enforcement every day on legitimate investigations. This cooperation can only occur through an appropriate legal basis that takes into account the specificities of each case including the data subject's country of residence and the owner and location of the data (when applicable).

More modern and streamlined mutual legal assistance ("MLA") processes represent an important tool to obtain digital evidence without creating jurisdictional and privacy conflicts between different states. We also encourage devoting additional resources to process the ever-increasing number of MLA requests between the EU and third countries.

The idea that progress can be achieved by creating a secure standard online portal for request and responses concerning e-evidence is promising and should be further explored.

At an intra-EU level, we support the use of EU mechanisms such as the European Investigation Order ("EIO"), which will help streamline cooperation between law enforcement and judicial authorities across borders, but more work remains to be done to render such instruments as viable solutions. The EIO, for example, is not binding and not all EU member states have adopted the Directive.

More significantly, we remain concerned that the potential for such EU mechanisms will not be realised if Member States favour instead broad unilateral assertions of jurisdiction. EU mechanisms are meant to address the problem of conflict of law that many of our member companies are confronted with, but their utility is constrained by the divergent scope of jurisdiction across countries.

As discussions move forward in the coming months, we call on you to assess the options that are available in a judicious manner that will not lead to serious and unintended consequences including weakening the security measures now widely used by consumers and companies alike, such as encryption.

In that respect, we endorse the approach suggested by the Slovak Presidency, which acknowledges the need for practical measures rather than the adoption of legislation. We believe that any proposals requiring companies to undermine the integrity and security of their products, infrastructure and services would be detrimental for the technological innovation as well as for privacy and security of European citizens.

We agree with ENISA and EUROPOL that *"solutions that intentionally weaken technical protection mechanisms to support law enforcement will intrinsically weaken the protection against criminals as well, which makes an easy solution impossible."*[1]

We absolutely do not believe that improving access to evidence in cyberspace should be achieved through mandating that the data be located in a specific jurisdiction. What matters is effective access to data when needed in the context of investigations, prevention of crime and terrorism, or exercise of regulatory authority. These objectives can be achieved through less prescriptive means, such as modernized MLA processes and other international cooperative mechanisms. Data localization requirements, by contrast, restrict access of enterprises and residents to online services, as only large entities can afford the multiple data centers per country needed (for both storage and disaster recovery). As cloud computing becomes increasingly prevalent, such restrictions only hurt countries' ability to take advantage of the latest computing advances.

Responsible technology providers are ready to assist law enforcement in legitimate investigations, in ways that are consistent with protecting consumer privacy and the security of the network and that at the same time provide ample breathing room for innovation and allow for meeting legitimate customers' needs.

[1] Joint ENISA-EUROPOL statement on lawful criminal investigation that respects 21st Century data protection, 20 May 2016

Our companies support practical solutions through an integrated EU approach. We trust that those discussions will build on the Council's sensible approach on this topic from June 2016[2], and feed into the Commission's upcoming plan in mid-2017 to improve criminal justice in cyberspace.

We very much look forward to working with you, the law enforcement community and relevant stakeholders.

Sincerely,

John Higgins
Director General
DIGITALEUROPE

James Waterworth
Vice-President
Computer and Communications Industry Association (CCIA Europe)

Thomas Boué
Director General, Policy – EMEA
BSA | The Software Alliance

[2] Council conclusions on improving criminal justice in cyberspace, 9 June 2016