AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

European Commission public consultation on improving cross-border access to electronic evidence in criminal matters

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €2 trillion in 2016, directly supports more than 4.5 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Introduction

AmCham EU takes an active interest in the digital policies of the European Union, particularly in the context and interests of transatlantic trade and investment. We have contributed recently to the European Commission's consultation on Building a European Data Economy and support the EU's efforts to modernize the corresponding legal landscape. This process is necessary to achieve digital transformation of Europe and to build confidence in transformative technologies helping the European economy grow.

Cross-border access to electronic evidence in criminal matters is an area of law that remains unsettled, and we are encouraged that the European Commission is attempting to provide legal certainty with appropriate safeguards in this area. For important purposes of public safety in the course of criminal investigations, law enforcement authorities (LEAs) across Europe increasingly need digital evidence that is stored or managed in different jurisdictions. In such circumstances, however, the fragmented laws and inconsistent protections of data belonging to individuals and organizations in different jurisdictions causes uncertainty and lack of trust in the digital economy.

As the Commission has worked to promote the free flow of data within the EU, and eliminate data localization laws that prohibit free flows of data in the cloud, the lack of certainty and safeguards relating to law enforcement access to electronic data more generally also need to be addressed to promote the Digital Single Market as well as transatlantic trade. The current situation inhibits the flow of data and encourages data localization among European technology users, in the private as well as public sectors, when they believe that their data is safer within their own countries. Moreover, the perceived difficulties for law enforcement to obtain certain types of digital evidence across borders causes some to seek data localization laws so that evidence is within their reach. A modern EU legal framework that ensures consistent protection of technology users while providing clearer and efficient law enforcement procedures would benefit the Digital Single Market and also pave the way towards a better transatlantic approach. Furthermore it must be considered that the increasing prevalence of cloud based services has in fact opened up a lot more data to be directly available upon request rather than previously where such data needed to be obtained potentially from the home or business of an individual via a search warrant or court order

AmCham EU is responding to relevant parts of the Commission's public consultation questionnaire on this topic. Because the questionnaire is primarily directed towards law enforcement authorities and service providers, we supplement our questionnaire response with these comments. As AmCham EU represents companies across sectors, these comments represent the views of technology users as well as providers.

Digital Evidence Initiatives in the EU

A vital step towards a coherent transatlantic framework would be a more harmonized approach within the European Union. Concerns about the problems of obtaining digital evidence across borders within the EU were raised in the 2015 European Agenda on Security. In June 2016, the European Commission

set up an expert consultation process to identify possible solutions, seeking input from various stakeholders including service providers, Member States practitioners and civil society organizations.

In June 2017, the Justice and Home Affairs Council reviewed options presented by the Commission to address these concerns. These options include: improving cooperation among judicial authorities (including via Mutual Legal Assistance procedures); improving cooperation with cloud service providers via practical measures that can be taken within the framework of current law; and proposing legislative solutions at the EU level to enhance the rule of law in this area.[1] With the support from the large majority of Member States, the Council requested that Commission pursue these options, and asked that a legislative measure be proposed by early 2018. The Commission has initiated an impact assessment and the current public consultation.[2]

The European economy will benefit if the service provider industry and customers operate within a clear legal framework that defines the limits and safeguards that govern when and how foreign governments may obtain data lawfully. LEAs will also benefit from legal clarity, so that investigations can proceed. The current EC process presents an opportunity for appropriate reform within the EU, as a step towards transatlantic solution.

To create a modern international legal regime that enables lawful access to data and also respects sovereign national interests, data protection and confidentiality, and the digital economy interests at stake, the EU and also the US have a strong mutual interest to find solutions to modernize and clarify the law. AmCham EU agrees that:

- The traditional regime of Mutual Legal Assistance Treaties (MLATs), originally designed for gathering physical evidence abroad, is under stress in today's digital environment and impractical for LEAs; and
- Jurisdiction over data based on traditional principles of territorial sovereignty is also impractical in many cases.

However, the MLAT regime included due process safeguards and protections for sovereign interests, which must remain strong elements of any new regime.

Access to evidence through direct cooperation with service providers

The Commission's e-evidence initiative seeks input on ways to improve direct cooperation between LEAs and digital service providers as a means to obtain evidence across borders. Direct cooperation with digital service providers can add value in criminal investigations, but is only appropriate under a clear rule of law that provides safeguards respecting individual privacy and organizational confidentiality interests. In cases involving organizations, direct cooperation with the organization,

[1] "Improving Cross-border Access to Electronic Evidence: Findings from the Expert Process and Suggested Way Forward," Commission services, 22 May 2017.
https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf

[2] "Inception Impact Assessment: Improving cross-border access to electronic evidence in criminal matters,"
https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3896097_en; "Public consultation on improving cross-border access to electronic evidence in criminal matters," 4 August 2017. https://ec.europa.eu/info/consultations/public-consultation-improving-cross-border-access-electronic-evidence-criminal-matters_e

rather than a service provider, is the most appropriate approach. Indeed the Commission acknowledges in its inception impact assessent that the current voluntary disclosure system with US service provides for non-content data for non-content data has been efficient.

In the vast majority of cases, LEAs in criminal investigations seek from service providers data relating to individual suspects, and data for which the service provider is the data controller. Digital service providers, as data processors, increasingly process and store data that belongs to all kinds of customers, including enterprises and public sector agencies – customers who remain the data controllers, with their own legal responsibilities to manage personal data in their possession as well as their own confidential and commercial information. In the case of organizations who are data controllers and merely use digital service providers as processors, law enforcement authorities should be required to cooperate directly with the data controller, not the processor.

The European Parliament included a chapter on e-evidence in its recent Report on Fighting Cybercrime, and identified this same issue when it stated that the Parliament:

> **"Stresses the need for any e-evidence framework to include sufficient safeguards for the rights and freedoms of all concerned; highlights that this should include a requirement that requests for e-evidence be directed in the first instance to the controllers or owners of the data, in order to ensure respect for their rights, as well as the rights of those to whom the data relates (for example their entitlement to assert legal privilege and to seek legal redress in the case of disproportionate or otherwise unlawful access); also highlights the need to ensure that any legal framework protects providers and all other parties from requests that could create conflicts of law or otherwise impinge on the sovereignty of other states." 3**

The Commission's questionnaire seeks little input regarding the interests of data controllers, or the potential impact of cross border access to data by LEAs on the digital economy. Any new EU legal framework should enhance the rule of law in a manner that increases confidence and trust in the Digital Single Market.

Organizations and public sector agencies typically control where their data is stored, and they need to be able to trust that they have the same rights when storing data in another country in the EU with a service provider providing services across the EU. A rule that ensures that any demands for digital evidence from data controllers comes directly to them will reassure such entities that the types of direct cooperation between LEAs and service providers contemplated by the Commission will still respect the rights to which such entities are entitled when data is stored on their own premises.

International Dimension

If the EU wishes to institute a system different than Mutual Legal Assistance Treaties to manage requests for digital evidence across borders, this can only be done by international agreement. The Commission's current initiative can ensure such agreement among Member States within the EU, and this is an important step. However, the Commission should avoid any unilateral attempt to assert extraterritorial jurisdiction outside the EU, regarding access to data stored exclusively outside the EU, without agreement of relevant third countries. Any such effort will only amplify conflicts of law and

[3] *Cite full title of report,* (para. 65) *[check against final report]*

encourage third countries unilaterally to assert jurisdiction over data that is subject to the protections and obligations of European law. The development of a common EU-wide approach should be a step towards a more coherent multilateral approach with third countries like the United States.

Ultimately, a modernized arrangement with the United States is needed for cross-border cooperation on digital evidence to replace the current MLAT structure. The need for digital evidence by LEAs on both sides is increasing, and frustration with MLAT procedures is causing countries to overstep jurisdictional bounds to seek access to digital evidence. Some countries, including the United States, seek quicker access to digital evidence by unilaterally claiming authority to seize it regardless of where it is stored and regardless of the sovereign rights and interests of other countries. To try to establish its extraterritorial authority, the US government has brought a series of cases against global cloud providers.[4] Litigation like this demonstrates the conflicts inherent in the current situation, underscoring the need for an updated system based on agreement between the EU and the US to define a rule of law that protects relevant interests while defining the capabilities of LEAs to perform their functions.

The EU can and should participate in actively seeking international agreement in this area, so that European citizens can rely on the rule of law governing data centres in Europe, and European LEAs also have greater ability to request content data from the US. A coherent legal framework within the EU is an important step in this direction. For this reason, AmCham EU is encouraged by the current initiative to improve cross-border access to electronic evidence in criminal matters, provided the interests and safeguards discussed herein are addressed.

[4] See, e.g., In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation (2nd Cir. July 14, 2016); In re the Search of Content That Is Stored at Premises Controlled by Google (N.D. Cal. Apr. 19, 2017); In re the Search of Premises Located at [Redacted]@yahoo.com (M.D. Fla. Apr. 7, 2017); In re the Search of Info. Associated with [Redacted]@Gmail.com That Is Stored at Premises Controlled by Google, Inc. (D.D.C. June 2, 2017); In re Search Warrant No. 16-960-M-01 to Google (E.D. Pa. Feb. 3, 2017).