AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

European Commission proposals on cross-border access to electronic evidence

Shaping the path for a modern legal international framework

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

Executive Summary

- Members of the American Chamber of Commerce to the EU (AmCham EU) understand the importance of effective cooperation with law enforcement authorities in accordance with the procedures and safeguards established by the applicable laws. The proposals presented by the European Commission on cross-border access to electronic evidence ('e-evidence') on 17 April 2018 can help further improve international cooperation on lawful access to data by establishing a transparent and principled EU-wide framework.

- Legislators should not lose sight of the international impact and the global precedent it is likely to set. In this regard, the suggested broad jurisdictional provision that goes beyond the international standard set by the Budapest Convention is concerning. A better solution is the inclusion of a proposal that would allow the EU to negotiate agreements with partners with comparable rule of law standards.

- The proposed Regulation on cross-border access to e-evidence ('the Regulation') includes a number of robust safeguards to protect the fundamental rights of users. We welcome the proposed procedural safeguards that allow providers to challenge the requests on legitimate grounds. In addition, requirements on transparency around demands by Law Enforcement Authorities (LEAs) for data help providers protect the fundamental rights of their users. Both must at least be preserved during the legislative process, and can be further improved.

- Furthermore, the requirement for LEAs to seek data in the first instance from the enterprise customer itself is essential to ensure that enterprises can comply with their obligations to process data in their care in compliance with EU law.

- The procedures and safeguards foreseen to handle potential extra-territorial conflicts with foreign law provide some protection for both users and providers and can help ensure that sovereignty and other compelling interests of foreign states are addressed. While minor improvements can be introduced, it provides an important template for a broader international framework for dealing with legal conflicts created by cross-border demands for data.

- It is essential to include an immunity for good faith compliance into the legal provisions of the proposal. The Regulation and Directive require service providers to comply with the European Production and Preservation Orders ('EPOs') and other legal processes, or face substantial penalties. However, they do not clearly protect providers if their compliance violates other EU or Member State laws.

- The Regulation should also be amended to give providers sufficient time to meaningfully evaluate, and respond appropriately to, each disclosure order they receive. In addition, the time limit for emergency cases, if any, should be aspirational as opposed to mandatory. They should be also limited to cases clearly defined by law, i.e. when there is an immediate threat to life or physical integrity, and not left to each officer to define.

- Other important aspects which need to be added in the Regulation are a mechanism to address conflicts with Member State law(s) and provider participation in conflict-of-law evaluation. It is also important that a review mechanism is available to ensure that within and between Member States reliance upon emergency requests does not become a routine request route.

Introduction

The American Chamber of Commerce to the EU (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. Our members represent a variety of industry sectors serving businesses and consumers across the EU. As industries across the world and specifically those in the EU increasingly leverage new technologies to transform their operations, regulatory policy addressing new technological challenges is increasingly cross-sectoral. Member companies invest heavily in technologies and processes designed to protect the security and confidentiality of their users' and customers' data, which may be increasingly stored and processed in the cloud.

Cross-border access to electronic evidence in criminal matters is an area of law that is still unsettled, and we have been encouraged by the European Commission's efforts to attempt 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.

While our members recognise the role and responsibilities of industry players in this space, we also firmly believe that LEAs must follow clear rules and procedures that fully safeguard users' privacy and other fundamental rights – especially in cases where evidence is stored in a different jurisdiction and production would implicate the interests of foreign citizens or governments. The rules governing law enforcement's ability to demand cross-border access to data hold by online service providers and stored in the cloud are therefore of paramount importance for AmCham EU.

Having clear rules that protect users' fundamental rights is an essential component of trust in online or cloud-based services. Users will be hesitant to use these services if they think the confidentiality and security of that data is at risk. As communicated in AmCham EU's earlier response to the Commission's public consultation[1], the European economy will benefit if the service provider industry and its customers operate within a clear legal framework that defines the limits and safeguards that govern when and how foreign governments may obtain data lawfully.

Accordingly, we believe the Commission's proposed electronic evidence ('e-evidence') package published on 17 April 2018[2] is an important step forward. The proposals establish a transparent and principled EU-wide framework that enables LEAs pursuing criminal investigations in one Member State to obtain digitally stored evidence where the provider or the evidence is located in a different Member State. It also includes a number of critical safeguards, to ensure that the fundamental rights of users are respected. As such, the proposal moves the EU closer to creating a more consistent and rules-bound international framework for lawful access to data in the cloud.

[1] See AmCham EU position paper 'European Commission public consultation on improving cross-border access to electronic evidence in criminal matters' http://www.amchameu.eu/position-papers/position-paper-european-commission-public-consultation-electronic-evidence (retrieved on 16 May 2018)

[2] See press release 17 April 2018: http://europa.eu/rapid/press-release_IP-18-3343_en.htm (retrieved on 16 May 2018)

As these proposals have already attracted substantial international attention, they are likely to set strong international precedents. The proposal can thus create a framework for a greater focus on the rule of law and fundamental rights safeguards, but could also fundamentally jeopardise such frameworks by undermining the protective role the Mutual Legal Assistance treaty protections serve in the international context. The suggested broad jurisdictional provision that goes beyond the international standard set by the Budapest Convention is concerning as it risks setting an unfortunate international precedent whereby States can seek to exert extra-territorial jurisdiction based on the availability of a service in that jurisdiction.

It is important that standards like possession and control and meaningful links to the requesting authorities' territory are retained and reinforced. It is also important to strive for government-to-government solutions when it comes to dealing with companies established outside the EU. The EU and also the US have a strong mutual interest in finding solutions to modernise and clarify the law that enables lawful access to data. We strongly encourage the legislator to reconsider the proposed jurisdictional rules in this global perspective and recommend to complement the proposal by government-to-government solutions, such as a potential EU-US agreement.

With the aim of supporting a modern international legal regime, this paper includes comments on key aspects of the proposal.

Key aspects of the proposed package

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 modernise and clarify the law. As such, AmCham EU would like to draw attention to the following key aspects of the Commission's proposal:

- **Clear jurisdictional rules that would set a positive international precedent** (Article 1 of the Regulation): The Commission proposal suggests that 'offering services in the Union' is by and large enough for any authority from any EU country to request data from any entity that belongs to the provider. This disregards two important international standards, also recognised by the Budapest Convention, namely the requirement that the service provider to whom the request is presented is in 'possession or control' of the requested information, and that there is a link to the territory of the country whose authority is requesting the information. In practice, this could mean that e.g. a Spanish authority can request data from a Hungarian provider, even if there is no Spanish user involved and the provider does not provide services in Spain. We assume this is not intended and would welcome clarification in this regard.

- **Respect for government-to-government solutions:** AmCham EU believes that a better solution than extra-territorial rules is to respect the current international standards and include a provision in the proposal that would allow the EU to negotiate agreements with partners with comparable rule of law standards. If this is not explicitly provided for it appears

difficult to square the obligations with the equivalent of an Article 48 provision of the GDPR if this was replicated in a third country in which a service provider was established. We would very much welcome the views of the Commission on how the standards introduced by the GDPR could be equally respected if replicated by a third country.

- **Robust protections for the rights of users** (Articles 4 and 5 of the Regulation): The proposed Regulation includes a number of robust safeguards to protect the fundamental rights of users. For example, the Regulation makes it clear that orders for the production of digital data (known as 'European Production Orders', or 'EPOs') can only be issued by a competent authority and must be validated by a judge, court, or prosecutor. For EPOs seeking more sensitive data (i.e. the content of a communication or its source or destination), only courts or judges can issue them, and the underlying crime must be serious. EPOs must also be no broader than necessary (i.e., 'necessary and proportionate') and are barred where the issuing LEA believes the data is protected by immunities or privileges in the Member State of the service provider or where disclosure would impact the national security, defense, or other fundamental interests of that Member State. These protections are vital to protecting user rights and must be preserved during the legislative process.

- **Including material safeguards**: Under the US system there are both procedural (i.e. who shall issue a given production order) and material safeguards (i.e. proof that the information requested is necessary for the case). Accordingly, if the US authorities request to issue a subpoena, they need to prove that the request information is 'relevant and material to an ongoing criminal investigation'. If they would like the court to issue a warrant, they have to meet the relatively high burden of proof: demonstrating 'probable cause' to believe that contraband or certain information related to a crime is present in the specific place to be searched. The EU system, as proposed by the Commission, only has procedural safeguards, which could be complemented with material safeguards, similar albeit not necessarily identical to the US system.

- **Notice** (Article 11 of the proposed Regulation): The Regulation recognises that in some scenarios EPOs must be kept confidential; however, in such cases, the Regulation also requires that the authority notifies the person whose data is being sought without undue delay once notification would no longer obstruct the relevant criminal proceedings. The authority must also provide information about available legal remedies. These requirements ensure there is transparency around LEA demands for data, which in turn helps cloud providers protect the fundamental rights of their users. Again, we believe these protections must be preserved in the legislative process. In terms of improvement, we would recommend rephrasing the current Article 11, to allow for notification as a rule and prohibit it as an exception. We would also recommend considering specific time limits for how long notification can be withheld. Last, but not least, we would recommend ensuring that providers have the ability to challenge orders not to notify and explicitly allow this in Article 16.

- **Demands for enterprise data** (Article 5 of the proposed Regulation): Where an EPO targets the data of an enterprise customer, it requires LEAs to seek that data in the first instance from the enterprise itself. LEAs can serve orders on cloud providers for enterprise data *only* where directing the order to the enterprise itself would not be appropriate, in particular because doing so might jeopardise the investigation. This requirement is essential to ensure that

enterprises – who will often be 'data controllers' under the EU's General Data Protection Regulation (GDPR) – can comply with their obligations to process data in their care in compliance with EU law. Furthermore, it should be clarified further that data needs to be provided only to the extent it is readily accessible to the recipient of the order. This would take into account technical limitations (such as encryption, Infrastructure as a Service (IaaS) access restrictions, etc.) as well as legal aspects (e.g. group structure and legal entity set-up)[3].

- **Clear rules on handling conflicts with foreign law** (Articles 15 and 16 of the proposed Regulation): Today, electronic data is often stored across national borders which improves the efficiency and resilience of information systems. It also means that when LEAs demand data, that data may be located in countries outside the Union and its disclosure might violate foreign law. The Regulation establishes two separate procedures through which a provider can challenge an EPO on these grounds. It also contemplates in certain situations that an EU court can notify authorities in foreign countries of the demand and give them an opportunity to oppose it.

  However, the access order remains valid when the foreign country authority fails to react within the proposed deadlines. While this may represent a procedural safeguard, it is important to recognise the volume of requests that will likely trigger this procedure. It will be paramount to find ways to ensure that the system remains workable. For example, asking the intervention of foreign authorities could become optional for the courts, in case they don't have other resources to establish the conflict. The legislation could also recognize previous interventions in similar cases.

  Overall, these safeguards provide some protection for both users and providers. They also ensure that LEA demands for data address potential conflicts in a responsible way that respects the sovereignty and other compelling interests of those foreign states that might be impacted by the disclosure. These procedures also provide an important template for a broader international framework for dealing with legal conflicts created by cross-border demands for data.

- **Clear scope** (Article 1 of the proposed Regulation): The Commission is to be commended for the proposal's clear scope. It covers only stored data (not data in transit) and does not empower Member State authorities to obtain direct access to service providers' systems. While Article 1 states that the Regulation lays down rules under which a Member State authority may order a service provider offering services in the Union to produce electronic evidence, it notes that this is without prejudice to powers of authorities to compel service providers established on their territories to comply with similar national measures. While we would not question the right of Member State laws to regulate purely domestic situations, this could be problematic where such national laws have cross-border implications as this is the very essence of the problem the Regulation is trying to solve.

[3] For example, the NIS directive uses the following limitation in Section 16 para 4 : 'The obligation to notify an incident shall only apply where the digital service provider has access to the information needed to assess the impact of an incident against the parameters referred to in the first subparagraph.'

- **Immunity for good faith compliance:** The Regulation and the Directive require cloud providers to comply with EPOs and other legal process, or face substantial penalties. However, they do not clearly protect providers, nor provider guarantees that compliance with the EPO does not violate other EU or Member State laws Recital 46 of the Regulation states that providers should be immune from liability for their good-faith compliance with disclosure and preservation orders. This immunity is critical, and should be included in the Regulation's operative provisions. We believe this change should be one of the main priorities as the proposals move through the legislative process.

- **Time limits for responses** (Articles 9 and 10 of the proposed Regulation): Article 9 of the Regulation requires providers to transmit data to LEAs at the latest within 10 days upon receipt' of an EPO, and 'within 6 hours' in emergency cases. Providing scrict time limits does not take into account that providers only have limited resources to process large volumes of requests. As such they need to be able to prioritise according to the urgency.

  Furthermore to adequately protect their users' interests, providers will need time to assess the legal validity of each order and to prepare their response, and the time limits in Article 9 and the corresponding recital will often be too short for such purposes.

  It must also be noted that Article 9(1) allows LEA to request that the data is provided in a shorter period than 10 days where it 'indicates reasons for earlier disclsoure'. This provision creates an incentive for requesting LEA to always set a shorter period and similar to the concerns outlined in relation to emergency requests to allow a form of 'queue jumping'. This is in nobodys' interest and requires more specificty as to why such a shorter period can be set and why such a request would not then qualify as an emergcny request.

  The Regulation should be amended to give providers sufficient time to meaningfully evaluate, and respond appropriately to each disclosure order they receive. In addition, the time limit for emergency cases should be aspirational as opposed to mandatory, as it simply will not always be possible to react more quickly in such instances. It should also be limited to cases clearly defined by law, i.e. when life or physical integrity is subject to imminent threat. LEAs should not have further discretion over deciding what is an emergency, otherwise every case may become one. Given the impact such time limits have on the ability of service providers to conduct due diligence and defend their users' interests if needed, an important change legislators could make to speed up disclosures of such data is to provide protection from liability.

- **Mechanism to address conflicts with Member State law(s)** (Articles 15 and 16 of the proposed Regulation)**:** Articles 15 and 16 of the Regulation provide mechanisms for courts to address potential conflicts with third-country laws. Yet there is no mechanism to guide providers when compliance with an order would violate the laws of a Member State other than that of the enforcing State (i.e., the Member State where the provider receives the order). Such conflicts could arise in any case where the data subject is a national of a Member State other than the issuing or enforcing State. Providers should have the ability to challenge compliance with orders that create a risk of such conflicts.
  As per the above, the proposed mechanism does not address cases where a foreign country authority does not respond to a notification and the order remains valid. This needs careful consideration, as a failure to act not negate the conflict of law nor will likely shield a service provider for any potential liability.

- **Provider participation in conflict-of-law evaluations** (Articles 15 and 16 of the proposed Regulation): When a provider challenges an order on the basis that compliance would conflict with third-country laws, Articles 15 and 16 authorise the issuing Member State authorities to refer that decision to a Member State court for review. However, neither article gives providers the right to intervene in these proceedings. Provider participation will be important, as providers often will have information relevant to a court's determinations. A lack of provider participation could lead courts to rule based on incomplete understandings of the law or facts. Articles 15 and 16 should expressly authorise providers to intervene in these court proceedings.

- **Relationship with the US Cloud Act**: The 'Cloud Act' provides a basis for the US government to enter into agreements with foreign governments that would allow it to reach US data stored overseas and allow foreign governments who have an agreement with the US to seek information directly from US companies, without the need for a Mutual Legal Assistant Treaty (MLAT). The EU and the US need to enter into an agreement for the EU to be able to use the direct reach to US service providers under the Cloud Act. The EU proposal should also explicitly recognise the need to conclude such agreements when dealing with international partners. It would be also important to have further clarity that Cloud Act agreements will qualify as 'international agreement' under Article 48 of the GDPR.

- **Alignment with existing legislation, in particular GDPR**: The explanatory memorandum of the draft Regulation states that 'Personal data covered by this proposal is protected and may only be processed in accordance with the [GDPR]'. Nonetheless, potential overlaps with the GDPR, and other directives, need to be more adequately considered and flagged. It would be helpful, for example, to include a provision that puts the onus on the requesting party to establish that the request is GDPR compliant so that service providers do not have to defend their compliance.

Conclusion

The e-evidence proposals can provide a strong platform for the Commission to negotiate agreements with third countries that provide similar rules-based protections for users and providers when LEAs seek access to stored data on a cross-border basis. We strongly encourage the legislator to consider the proposed jurisdictional rules in this global perspective and recommend to complement these proposals by government-to-government solutions, such as a potential EU-US agreement. With the objective of creating a strong basis for a modern legal framework, we call legislators to maintain and strengthen existing safeguards and procedures for users and providers. Most importantly, an immunity for good faith compliance needs to be introduced for providers and time limits reviewed. Furthermore, while very importantly clear rules for handling conflicts with foreign law have been included, mechanisms to address conflicts of law need to be further developed.