AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Consultation response

AmCham EU response to the Roadmap on Police Cooperation – stronger mandate for Europol

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 U.S. positions on business matters. Aggregate U.S. investment in Europe totalled more than €3 trillion in 2019, directly supports more than 4.8 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

Executive summary

The American Chamber of Commerce to the European Union (AmCham EU) welcomes the opportunity to provide our views on the European Commission's roadmap[1] on strengthening the mandate of the European Union Agency for Law Enforcement Cooperation (Europol).

AmCham EU takes an active interest in the digital policies of the EU, including the field of cross-border access to electronic evidence (e-Evidence)[2] in criminal matters. We recognise the role and responsibilities of private companies in this space and many of our members have a strong working relationship with Europol. We view the agency as an important component to preventing and combatting criminal activity in the EU.

The below sets out our initial views and subsequent questions to the policy options set out by the European Commission (EC) in its roadmap. Our views focus specifically on 'Objective I – Enabling Europol to cooperate effectively with private parties'. We provisionally support 'Option 3 – In addition to the receipt of data set out in Option 2, allowing Europol to request data directly from private parties or query databases managed by private parties (eg, WHOIS) in specific investigations', provided that this operates on a voluntary basis and pending clarity on the issues set out below.

Cooperation with private parties on a voluntary basis

AmCham EU supports the view of Member States[3] that any future regime allowing for Europol to directly request data from private companies should be voluntary. The introduction of an obligatory data disclosure regime by private parties would be disproportionate and premature. This is particularly true in light of the on-going legislative discussions on the proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (e-Evidence Regulation)[4] as the EU institutions have yet to agree on a framework for providing such powers to national law enforcement authorities (LEAs).

We believe negotiations on the draft e-Evidence Regulation must not only conclude, but the effectiveness of the new framework must be properly assessed before providing Europol with equivalent powers.

Alignment with General Data Protection Regulation and ePrivacy Directive

AmCham EU welcomes the view of Member States[5] that any future regime governing the direct transmission of data by private parties to Europol should be in full compliance with fundamental rights and applicable legislation, in particular the General Data Protection Regulation (GDPR).[6] AmCham EU notes that any voluntary data disclosure from a private party to Europol will require a sufficient legal basis for transmission [… such voluntary data disclosure is provided for by the permissive legal bases of the GDPR; it is not provided for in the ePrivacy Directive (ePD)[7]]. Private parties must be provided the necessary time to assess each data request and not face undue pressure from Europol or national LEAs should a data request be rejected due to GDPR compliance concerns.

If the future data disclosure framework is obligatory in nature, then there needs to be a proper mechanism to address potential conflicts with third country laws similar to what can be found in the draft e-Evidence

[1] Ares (2020)25552019 – 14/05/2020

[2] https://www.amchameu.eu/system/files/position_papers/amcham_eu_position_e-evidence_package_final.pdf

[3] DOC 14745/19

[4] COM/2018/225 final – 2018/0108 (COD)

[5] Ibid

[6] Regulation (EU) 2016/679

[7] Directive 2002/58/EC

Regulation and common international comity law proceedings. In addition, where it is not possible to provide the information in the requested time, the information may be provided in phases without undue further delay, similar to what is provided in Article 33 of the GDPR.

Scope of crimes covered by data requests

Annex 1 of the current Europol mandate[8] sets out a long list of criminal activity for which the agency is competent. This ranges from terrorism to motor vehicle crime and computer crime to the illicit trafficking in endangered animal species. It remains unclear in the ECs roadmap whether Europol would have the ability to request data from private parties for all forms of criminal activity found within Annex 1 or whether only certain 'serious' crimes would allow for the agency to directly request data from private entities.

As existing and future EU legislation (eg, European Investigation Order Directive[9] and draft e-Evidence Regulation) in the field of judicial cooperation focus on serious crimes, we would encourage the future Europol mandate to set out a clear list of crimes whereby the agency could issue a voluntary data request. We encourage this list to focus on serious crimes that truly require the necessary cross-border coordination provided for by Europol.

Recipients of data requests

The EC roadmap does not specify which type of private companies would fall within the scope of a possible future voluntary data request from Europol. AmCham EU notes that Article 2 of the draft e-Evidence Regulation states that the future framework will only apply to:

1. Electronic communications services as defined in Article 2(4) of the EECC;

2. Information society services as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 for which the storage of data is a defining component of the service provider to the user, including social networks, online marketplaces facilitating transactions between their users, and other hosting service providers; and

3. Internet domain name and intellectual property (IP) numbering services such as IP address providers, domain name registries, domain name registrars and related privacy and proxy services.

AmCham EU questions whether the scope of the future Europol regime would be restricted to the same group of service providers set out in Article 2 of the draft e-Evidence Regulation or whether this would be extended to cover other service providers. We would add that authorities' requests for data which are made to service providers must be limited to data within the provider's control. If the data is only stored on a service provider's server, but is not controlled by the provider, the request for data should not be addressed to the service provider. In other words, data storage should not be the only condition for a service provider to be addressed with a data request.

Recent public comments made by the Commissioner for Home Affairs, Ylva Johansson, seems to indicate that entities within the field of financial services would also be covered by the future framework. We encourage the EC to provide further information on the scope of the future regime and would welcome the opportunity to provide the EC with further feedback on the potential impact of the inclusion of certain industry sectors.

AmCham EU also encourages the EC to clarify whether the future regime would mirror that of Article 3(3) of the draft e-Evidence Regulation whereby Europol would only be able to request data from entities which are providing a service offered in the Union. We would support such a scope of application as this would greatly

[8] Regulation (EU) 2016/794

[9] Directive 2014/41/EU

limit the possibility of conflicts with third country law, particularly the limitations set out in the US Stored Communications Act.[10]

Data covered

The EC roadmap does not specify which type of data the future regime would apply to. While the draft e-Evidence Regulation will cover both stored content and metadata, AmCham EU questions whether the updated Europol mandate would necessitate such an expansive scope. In light of the heightened sensitivity associated with stored content data, along with the limitations placed on US based service providers by US law in disclosing such data outside of a mutual legal assistance (MLA) request, we believe the future framework should be limited to stored metadata requests only.

Furthermore, the draft e-Evidence Regulation takes an innovative approach to defining stored metadata by creating three sub-categories ('subscriber', 'access' and 'transactional' data) while placing a higher threshold on requesting access to the latter. In an effort to ensure harmonisation, we encourage the EC to consider adopting a similar approach in the future Europol Regulation.

Increased resources

While AmCham EU members have a strong working relationship with Europol, many observe that the agency is often operating with restrained resources, impacting its ability to effectively fulfil its role. As the EC considers expanding the responsibilities of Europol, we believe this must be paired with a substantial increase in resources. Without a much-needed resource boost, Europol risks facing increased frustration from national LEAs and an erosion of the strong reputation it has built with private companies and the global law enforcement community.

[10] 18 U.S.C. §§ 2701 to 2710