DIGITALEUROPE

DIGITALEUROPE's response to the European Commission's public consultation on improving cross-border access to electronic evidence in criminal matters

Brussels, 25 October 2017

DIGITALEUROPE, the voice of the digital technology industry in Europe, welcomes the European Commission's public consultation on improving cross-border access to electronic evidence in criminal matters and the opportunity to provide feedback on the impacts of the proposed solutions. We have participated in the corresponding stakeholder workshops and continue to support the DG HOME-DG JUST task force effort to tackle the difficult jurisdictional and other challenges that must be resolved to develop a common approach in the EU. This paper largely reflects our previous submissions, and we want to contribute them formally in the context of this public consultation.

DIGITALEUROPE would like to reiterate that our members take their responsibility to maintain the safety, security, and privacy of millions of users in the EU seriously. Our members are also committed to being transparent in the way they execute these responsibilities.

As stated in DIGITALEUROPE's submission to the Commission's task force from 3 March 2017, our members recognise that there are situations where they need to assist law enforcement agencies carrying out investigations into criminal activity. However, they also acknowledge that the legal framework governing cross-border requests should be clarified, and we are eager to continue to work with all relevant stakeholders on these important issues.

In August 2017, the Commission published the Inception Impact Assessment that identified for consideration possible legislative solutions aimed at improving legal certainty, transparency and accountability regarding cross-border access to e-evidence in criminal investigations. The results of the assessment will feed into the legislative proposal that is to be presented by the Commission in early 2018. Additionally, the Commission's "non-paper" from June 2017 lists practical measures to improve cooperation with service providers within the existing legal framework. These practical solutions received approval of the JHA Council and are currently being implemented. As the public consultation process will inform the introduction of both legislative and practical measures, DIGITALEUROPE would like to emphasize points relevant to the consultation and add additional comments.

Regarding practical measures, DIGITALEUROPE strongly supports the European Commission's effort to find workable solutions to improve cooperation with service providers within the existing framework.

- We believe that 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.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

- An **online tool containing all the applicable national laws** as well as a description of who has authority to submit requests would also provide tangible improvements and contribute to a common understanding for all relevant stakeholders.
- DIGITALEUROPE members also strongly **support coordinated trainings and 'train-the-trainers' programmes** as well as other practical ways to achieve meaningful improvements in cooperation.
- Requests for access to data also need to respect **procedural safeguards and the rule of law**. Accordingly, any request must be "reasoned," based on law and subject to review and decision by a court or an independent administrative body; be limited to what is strictly necessary for the investigation in question, and target individuals implicated in the crime. Authorities shall also notify the user concerned and companies should have the ability to do so.

We welcome the fact that many of these suggestions were incorporated in the Commission's non-paper and that both the non-paper and the Inception Impact Assessment take into account the fundamental rights aspects of the disclosure of e-evidence.

Furthermore, any potential solutions should in no way lead to a requirement for a service provider to reverse engineer, provide back doors or any other technology mandates to weaken the security of its service. Service providers must have the ability to continue to deploy the best possible encryption technologies to ensure the security, integrity and confidentiality of their services. Such measures would only lead to a weakening of data security and privacy of the entire digital ecosystem.

DIGITALEUROPE has also expressed our support for the European Commission's efforts to **modernise international cooperation**, in particular the efforts to improve EU-US cooperation on cross-border access to e-Evidence and the dedicated funding of such initiatives.

- DIGITALEUROPE members strongly believe that in order to avoid conflicting laws, there should be a **robust, principled, and transparent framework to govern lawful requests for data** across jurisdictions, such as improved mutual legal assistance treaty ("MLAT") processes. Where the laws of one jurisdiction conflict with the laws of another, it is incumbent upon governments to work together to resolve such conflicts.
- The non-paper suggests **EU level bilateral agreements with key partner countries such as the US**. We encourage such efforts.

At the JHA Council in June 2017, the Member States clearly recognized the urgency and the necessity of the introduction of legislative measures and asked the European Commission to come up with concrete legislative proposals by the end of the year. While DIGITALEUROPE welcomes this assessment, it also calls upon the Commission and the Council to ensure that any measures towards a potential EU framework do not create an additional conflict of law situations. The EU should not attempt to authorize extraterritorial seizures of data controlled or entirely stored outside the EU. Cross-border data demands from the EU to the US, or vice versa, need to be resolved via international agreement, as mentioned above. Unilateral assertions of jurisdiction by either EU member states, or by the US, risk potential conflicts of laws, given the restrictions on data transfers or disclosures imposed on service providers by the Stored Communications Act in the US and the GDPR in the EU. Any extraterritorial reach of EU data seizure rules should anticipate that other nations could impose reciprocal rules to demand the data of Europeans in Europe, infringing on citizens' fundamental rights.

DIGITALEUROPE questions the option suggested in the non-paper and the Inception Impact Assessment for a legislative solution to facilitate direct access. In this context, we understand direct access to mean law

enforcement access to computer systems through a suspect's own device – so-called "legal hacking" – without the involvement of any service provider. Given the drastic nature of such measures and the likelihood of violating fundamental rights as well as sovereign interests of other nations, safeguards and limitations should be clearly spelled out to prevent misuse of "legal hacking." We have seen recently the serious issues that can arise from so-called software vulnerability stockpiling.

As mentioned above, any solutions found at EU level need to respect the rule of law and fundamental rights. The European Court of Human Rights and European Court of Justice jurisprudence should be taken into account.

Any solution to improving criminal justice in cyberspace must consider the need for users of cloud technology services—whether individuals, governments, or organizations—to be accorded the same protections for their e-evidence as for the information they commit to paper, including the right to be notified that their data is being accessed.

DIGITALEUROPE members are acutely aware that customers often do not want to put their data in a cloud infrastructure outside their national borders, partly 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 an individual or a user could contest the government's demand in the same way as they could before they had moved information to the cloud.

Any new framework must address this core concern and possible inhibitor to adoption of cloud technologies. Potential customers will naturally be reluctant to take advantage of cloud technology if they perceive that their privacy protections will be reduced by such technologies. These customers, as data controllers themselves, have direct legal obligations concerning the management of their data. They should be direct recipients of any law enforcement demands for data, not service providers.

The European Commission's December 2016 progress report stated that the rules on when a notice from service providers to customers has to take place vary widely or are entirely absent. A key component to any solution should, therefore, address the issue of user notification. Unless service providers are bound by a Court Order not to disclose a data request due to the fact that it would jeopardise the investigation, it is important that our members are able to notify users.

DIGITALEUROPE welcomes the work by the European Parliament on the issue and the recently adopted INI report on fight against cybercrime. The report clearly articulates Parliament's support for a coherent EU framework and improving law enforcement access to data, but only in accordance with data protection law and MLATs. Importantly, the report also acknowledges the rights of data controllers and owners, noting that "any e-evidence framework [...] 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."

Last, but not least, we regret to see that the ongoing consultation process does not acknowledge or mention the ongoing negotiations on the European Electronic Communications Code and the ePrivacy Regulation proposals, which touch many of the issues discussed above. It is essential that the EU strives for an integrated approach and holistic solution, as opposed to looking at the challenges in silos.

DIGITALEUROPE commends the European Commission for its work on the e-evidence initiative and remains committed to working with the Commission to find solutions to these challenging, but important questions.

--
For more information please contact:
Ramus Theede, DIGITALEUROPE's Policy Director
+45 29 90 80 30 or rasmus.theede@digitaleurope.org

ABOUT DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE's members include in total 25,000 ICT Companies in Europe represented by 61 corporate members and 37 national trade associations from across Europe. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

DIGITALEUROPE MEMBERSHIP

Corporate Members

Adobe, Airbus, Amazon, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Intel, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Cyprus: CITEA
Denmark: DI Digital, IT-BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Force Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: TECHNOLOGY IRELAND
Italy: ANITEC
Lithuania: INFOBALT
Netherlands: Nederland ICT, FIAR
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK