DIGITALEUROPE

DIGITALEUROPE's response to the European Commission's Progress Report on Improving Criminal Justice in Cyberspace

Brussels, 3 March 2017

EXECUTIVE SUMMARY

DIGITALEUROPE as the voice of the digital technology industry in Europe welcomes the on-going leadership of the European Commission in addressing the complex problem of global access to electronic evidence ("e-Evidence"). We 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.

As the European Commission noted in its December 2016 progress report[1], DIGITALEUROPE members remain key stakeholders in the continued discussions. **We 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.

DIGITALEUROPE members recognise that there are situations where they need to assist law enforcement agencies carrying out investigations into criminal activity. However, our members 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.

DIGITALEUROPE strongly supports the European Commission's effort to find practical and 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. 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. **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 also supports 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,

[1] Non Paper: Progress Report Following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace (December 2016)

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

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.

DIGITALEUROPE notes that the European Commission's progress report highlighted the many divergent approaches that Member States have taken on this delicate issue, including how to determine the exercise of jurisdiction over service providers to access e-Evidence. We agree that these divergent approaches have led to conflicts of law throughout the EU and internationally. We are encouraged that the task force has focused on this specific issue. **A common framework in the EU with robust safeguards protecting fundamental rights in line with the recent jurisprudence of the Court of Justice of the European Union ("CJEU") and the due process required by the Court will better serve all stakeholders**. While ultimately this problem must be resolved amongst governments, we nonetheless appreciate the opportunity to contribute to its resolution.

OVERALL VIEWS

The June 2016 Council Conclusions[2] focused on: 1) improving cooperation with US service providers under existing law; 2) streamlining government-to-government mutual legal assistance under current treaties; and 3) reviewing rules on 'enforcement jurisdiction' in cyberspace. DIGITALEUROPE fully recognises and supports the European Commission's work on these issues and will continue to work with the European Commission to achieve progress on these fronts.

In terms of prioritising, DIGITALEUROPE would like to highlight and encourage future European Commission activity on the following areas.

1. Finding practical solution to lawful access to data

DIGITALEUROPE welcomes the European Commission's approach to find practical and meaningful solutions to improve cooperation between service providers and law enforcement authorities. Many of the solutions identified by the European Commission, such as the creation of single points of contact on both sides, trainings, standardisation, reduction of forms, etc. are clearly measures that can lead to tangible improvements to the current situation.

When considering the establishment of an online platform to provide comprehensive guidelines, we strongly encourage the European Commission to also consider using this platform to collect all the relevant national legal requirements, such as the criminal codes, corresponding procedural and other requirements as well as their English translations. This would facilitate a common understanding of these rules among service providers and facilitate the dialogues with the national authorities. As the European Commission reported, it is not always easy to understand who has the authority to require information. The online platform could provide clarity on this as well.

Our members also often participate in training programmes, such as the recent programme organised at the *Ecole Nationale de la Magistrature* with the support of the EU, the Council of Europe and other stakeholders. **Streamlining training programmes could help ensure that resources are concentrated on efforts that deliver the most effective outcomes.**

[2] Justice and Home Affairs Council Conclusions on Improving Criminal Justice in Cyberspace (June 2016)

2. Identifying a common jurisdictional basis among EU Member States to find and develop workable solutions

It is clear that jurisdictional overreach represents an important challenge which cannot be ignored. The lack of a common approach could also be further exacerbated by other EU legislative developments, such as the proposed Regulation on ePrivacy which could potentially create more confusion, rather than clarity, in this space.

As the progress report indicates, the jurisdictional criteria enabling law enforcement to make such requests vary, ranging from the 'main seat of the service provider' (in 16 Member States), 'the place where services are offered' (in 6 Member States), to 'the place where data is stored' (in 6 Member States), and a combination of alternatives. This lack of a common approach often leads to conflicts of law throughout the EU. DIGITALEUROPE members are not alone in dealing with these conflicts in Courts throughout the EU. **Given the nature of e-Evidence, which transcends traditional notions of territorial jurisdiction, identifying a common jurisdictional basis among Member States will be critical to finding a workable solution**. We, therefore, appreciate the opportunity to provide feedback on the scope and basis for jurisdiction to protect data from disclosure and/or compel its disclosure to law enforcement.

Cybercrime is a global phenomenon and as such, conflict of laws remain a challenging problem within the EU and at the international level. It is, therefore, important to develop a robust, principled, and transparent framework to govern lawful requests for data across jurisdictions, such as improved MLAT processes and ensure that these instruments are truly relied upon when requests for data creates a conflict of law.

3. Respecting fundamental rights

Any solutions found at EU level need to respect the **rule of law and fundamental rights**. The jurisprudence from the European Court of Human Rights ("ECHR") and the CJEU should be taken into account.

For example, the CJEU underlined that access of the competent national authorities to data should only be allowed where the objective pursued by that access, in the context of fighting crime, is subject to prior review by a Court or an independent administrative authority, and where it relates to the individual concerned.

4. According same protections to users of cloud technology services including the right to be notified when their data is being accessed

Many companies across various industry sectors are today using cloud-based infrastructure to deliver applications and services to customers resulting in substantial cost-saving and efficiency gains. To foster growth and innovation in the EU digital economy, DIGITALEUROPE continues to encourage the adoption of these technologies. We believe that is it of fundamental importance to better understand the decision-making factors for individuals, governments or organisations who are deciding whether to adopt these changes.

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 in part 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 for their information committed to paper.

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.

The European Commission's progress report states that the rules on when notice 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.

CONCLUSION

DIGITALEUROPE notes that the European Commission will be making recommendations to the Council in advance of the June Justice and Home Affairs Council. DIGITALEUROPE is looking forward to working with the European Commission to find solutions to these challenging, but important questions.

--

For more information please contact:
Damir Filipovic, DIGITALEUROPE's Director (Digital Consumer and Enterprise Policy)
+32 2 609 53 25 or damir.filipovic@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 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

Airbus, Amazon Web Services, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Intel, iQor, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, 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, 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