**Flash report – 19 June 2017 roundtable meeting with service providers, industry associations and civil society organisation on cross-border access to electronic evidence and on the role of encryption in criminal investigations**

The roundtable meeting was organised in relation to the EU Internet Forum.

Cross-border access to electronic evidence

The roundtable meeting was organised to give service providers, industry associations and civil society organisations the opportunity to react to the Commission's non-paper presented at the 8 June 2017 Council meeting and the Technical Document on cross-border access to e-evidence, which summarise the findings of the expert consultation process. Three written contributions were submitted before the meeting: from Microsoft, Access Now and Digital Europe.

To start the meeting, COM briefly presented the content of the non-paper and the different practical measures and legislative options proposed. Access Now and Digital Europe then briefly presented their main comments contained in their written contributions. Both welcomed the transparent expert consultation process and the need for reforms as regards the channels for cross-border access to e-evidence.

For Access Now, MLA should remain the main channel to obtain e-evidence in order to ensure appropriate human rights safeguards, and the relationship between the new legal instrument for production requests/orders and the EIO was questioned. Other channels should remain the exception. The scope of electronic evidence was questioned as well as the reason for differentiating between digital and physical evidence. Digital Europe welcomed practical measures, but stressed that any legislative initiative should not create additional conflicts of law and should be consistent with the proposal for the e-Privacy Regulation, and reminded that cross-border access to data was an increasingly important concern for customers of cloud services. Both associations expressed concerns with regard to direct access. Access now raised human rights concerns, but indicated they would welcome harmonised rules if complemented with the rights human standards. Digital Europe enquired about further details of possible measures on direct access.

No participant had any comment regarding the problem definition.

On practical measures, one participant inquired whether the US Department of Justice supported the practical measures concerning the US. Participants also presented their views on the possible legislative reform in the US. COM explained the good bilateral relationship with the US, on the basis of which regular discussions on e-evidence also take place.
Another participant wondered whether streamlining of providers' policies could be achieved in view of the different types of data and different architectures service providers are working with, but saw potential for streamlining the request mechanism, and referred to the example of France where this had been done.

On legislative measures the different options considered in the non-paper were discussed. Regarding the production order/request, several participants pointed out that the measure of the legal

representative would not solve conflicts of law with the US regarding content data, as ECPA prevents providers with headquarters in the US to disclose it to foreign law enforcement. The same conflict would currently still exist for a provider headquartered in the EU but who saves its data in the US (save for emergency requests). COM acknowledged that the legal representative alone would not address conflicts of law, for which other measures, including bilateral or multilateral agreements could be considered. The non-mandatory nature of production requests would also prevent conflicts of law.

One participant pointed out that user notification was an important issue for them, which should be addressed by a proposal. Moreover, it was suggested that sometimes a customer may be considered as the data controller for the processing of personal data, and not the service provider, raising the question as to whom the order should be addressed. One participant inquired which types of data would be covered by the production order and the production request, and whether there was a difference in scope. Regarding the scope, participants wondered whether the focus would be on "Internet Service Providers", or go beyond, e.g. also covering banks. Why should different economic sectors be treated differently? COM indicated that follow-up work will be necessary to determine several parameters, e.g. on types of data and definitions of service providers.

Regarding direct access, many participants had questions or strong concerns, as they view any access of authorities to data via "hacking" as unlawful. It was suggested that even by providing a framework with common safeguards to address cross-border effects of direct access, the EU would endorse these practices. One participant pointed out that data stored on a computer that could be accessed through such measure was not limited to electronic communication data but much broader. Another participant observed that a service provider would not be able to distinguish software installed by law enforcement authorities from criminal malware.

On the follow-up to the 8 June 2017 Council meeting, COM committed to consulting stakeholders on a work plan for the implementation of practical measures, including on the cooperation with service providers. An Inception Impact Assessment for possible legislative measures will also be published in due time.

The role of encryption in criminal investigations

The roundtable meeting was also used to present participants an update on COM's work on the role of encryption in criminal investigations and to provide an opportunity to consider issues in relation to a number of approaches used by law enforcement authorities to address encryption challenges.

COM gave a presentation on the process set up to engage with stakeholders, establish a problem definition and assess options for further action in relation to the role of encryption in criminal investigations. COM welcomed the opportunity to exchange views with relevant stakeholders and explained the intention to provide for additional opportunities for stakeholder to provide input.

In response to the presentation, one participant enquired about the existence of empirical data on the issues encountered by authorities, in response to which COM clarified that the current process is established to build an evidence-base for possible further actions. On possible further actions, COM underlined that it recognises the importance of strong encryption for the protection of cybersecurity

and personal data. COM clarified that it is currently not planning on proposing legislation, but that all relevant options for action will be considered as part of the process. COM indicated that it is too early to present specific options as the process is still ongoing. One participant underlined the need to take into account that encryption workarounds for law enforcement authorities can also be employed by criminals.

As a basis for the discussion on approaches used by law enforcement authorities to address encryption challenges, COM presented a 2017 paper by Kerr and Schneier on encryption workarounds. On approaches that relate to "finding an encryption key", participants stressed limitations as often it is only the target that knows the key, i.e. service providers often cannot assist authorities when end-to-end encryption is used. One participant underlined the need for sufficient safeguards, e.g. when finding a key involved measures to search someone's house. Reference was also made to the possible use of social engineering practices.

On approaches that relate to "guessing an encryption key", service providers again stressed limitation as often it is only the target that knows the key, i.e. service providers often cannot assist authorities when end-to-end encryption is used. One participant suggested that the use of weak passwords might provide for opportunities for authorities to guess a key, but another participant warned about possible impact on performance of online services for these approaches. Other participants explained that they notify customers when they have indications that someone has been attempting to guess a password or key, for which they cannot make a distinction between law enforcement authorities or cybercriminals.

On approaches that relate to "compelling a key", participants argued against the introduction of legal obligations for service providers to produce an encryption key. They stressed that it is often only the target that knows the key, i.e. service providers often cannot assist authorities when end-to-end encryption is used. Participants stressed that they often do not have and do not know a key. They cannot generate an additional key without weakening the use of encryption for a particular service. One participant stressed that an obligation for a target to produce a key could interfere with the right against self-incrimination that is recognised in many countries' legal framework. The Commission enquired about different approaches under Member States' legislation vis-à-vis providers of electronic communications services and providers of information society services, in response to which one participant indicated that many providers of Over-The-Top (OTT) services employ end-to-end encryption for their services.

On approaches that relate to "exploiting a flaw in an encryption scheme" participants argued for an obligation to report 0-day vulnerabilities by law enforcement authorities in view of the impact of their use from a cybersecurity perspective. One participant stressed that 0-day vulnerabilities can also be used by criminals. Another participant indicated that attempts by authorities to include vulnerabilities in encryption schemes have seriously affected their credibility in the past. One participant argued for the development of policies on responsible disclosure of 0-day vulnerabilities. Following a discussion it was recognised that already knows ("old-day") vulnerabilities can also be used by authorities as an encryption workaround.

On approaches that relate to "access to plaintext on a device" participants underlined the possible impact on fundamental rights and argued for sufficient safeguards. One participant elaborated on the use of software by law enforcement authorities to obtain access to plaintext on a target's device,

indicating that this cannot be distinguished from malware used by criminals. Following a discussion it was recognised that different approaches can be used to obtain access to a plaintext version of encrypted information, e.g. as part of an extended search or as part of a remote search.

On approaches that relate to "locating a plaintext copy", one participant that law enforcement authorities may have to consider appropriate procedures based on mutual legal assistance to obtain a plaintext copy. Another participant pointed at transparency reporting by service providers, as part of which law enforcement authorities' request will be reported on.