DIGITALEUROPE

15 NOVEMBER 2019

eEvidence Scope

Scope (Arts 1, 3 and 23)

Material scope

DIGITALEUROPE agrees with both the Commission and the Council positions which restrict the scope of the e-evidence package to stored data, excluding real-time interception and 'direct access.' DIGITALEUROPE urges the European Parliament to do the same.

Exclusive use of Union instruments for cross-border situations

When law enforcement authorities seek data from a company whose main establishment is located outside of the requesting authority's country, the e-evidence package preserves mechanisms that many law enforcement authorities (LEAs) rely on today to obtain data on a cross-border basis, including through European Investigation Orders (EIOs) and orders obtained through Mutual Legal Assistance (MLA) ('Union measures'). The e-evidence package also preserves the use of national orders for purely domestic scenarios.

Art. 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 clarifies, however, that this is without prejudice to authorities' powers to compel service providers established on their territories to comply with similar national measures. While we do not question the right of Member State laws to regulate purely domestic situations, that should not be the case where such national laws have cross-border impacts as this is the very essence of the problem the Regulation is trying to solve.

It is unfortunate that the Council's General Approach does not impose any obligation on an issuing authority to use a European Production Order (EPO) or European Preservation Order (EPO-PR) over a domestic instrument in cross-border cases – a shortcoming it shares with the European Commission text. As a result, the Council's text allows LEAs to bypass the safeguards set out in the

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

proposed package and other Union measures and instead use a purely domestic legal process to obtain data about users located in a different Member State.

Such domestic procedures might offer fewer safeguards and result in weaker protections for fundamental rights across the EU. This approach also runs counter to the proposal's fundamental harmonisation goal, as service providers will be required to examine, and process orders based on different legal bases.

We urge the European Parliament to require LEAs to use EPO(-PR)s or other Union instruments over domestic procedures unless those instruments are applicable. Revising the proposals in this way will strengthen safeguards for fundamental rights and reduce the risk that LEAs, using domestic procedures, will impose demands on service providers that can circumvent these safeguards.

Jurisdiction

We are concerned that both the Commission's proposal and the Council's General Approach depart from the standard of jurisdiction established by the Budapest Convention. That standard is composed of four elements, including the requirement that the service provider has possession and control over the requested information, which is missing from the e-evidence package.[1]

Companies should be able to maintain robust internal procedures that limit access and disclosure rights to users' communication data to those company personnel who are best placed to conduct the task.

Sales personnel in a store that sell hardware, for example, who may or may not be full-time employees and have no reason to access user information such as their emails, should not be punished for their inability to comply with the Order. Recognising the standard based on possession or control should not inhibit effective cooperation, as EPO(-PR)s will help authorities address the relevant

[1] See pages 13-14 of the study Commissioned by the LIBE Committee 'an assessment of the Commission's proposal on electronic evidence' (http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2018)604989)

European entities. However, the standard is essential from an international and data protection perspective.[2]

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Senior Policy Manager for Infrastructure, Privacy and Security

alberto.difelice@digitaleurope.org / +32 471 99 34 25

[2] It is also important that this standard is also preserved in the context of the 2nd Additional Protocol to the Budapest Convention.

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 Membership

Corporate Members

Airbus, Amazon, AMD, Apple, Arçelik, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Epson, Ericsson, Facebook, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, MasterCard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, Visa, VMware, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: Nederland ICT, FIAR
Norway: Abelia
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