DIGITALEUROPE

DIGITALEUROPE views on Law Enforcement Access to Digital Evidence

Brussels, 17 October 2016

EXECUTIVE SUMMARY

DIGITALEUROPE as the voice of Europe's digital technology industry expresses its willingness to work closely with the EU Institutions and policymakers as they decide how to address law enforcement access to digital evidence. We welcome that the EU Institutions have recognised that current rules and practices regarding digital evidence have created some uncertainty among customers, providers, and law enforcement authorities. As policy makers continue to investigate potential solutions, DIGITALEUROPE believes any future actions should focus on:

- Clear rules – Agreement on the rules governing law enforcement access to data for purposes of public safety, data protection and economic growth.
- Involve all stakeholders – Efforts of the European Institutions to improve criminal justice in cyberspace must take into account the views and rights of all stakeholders, especially individuals.
- Modernisation of rules – The multijurisdictional nature of internet services requires the modernisation of procedures regarding one country's access to data controlled in another country.
- Avoid unilateral actions – Unilateral efforts to seize data across borders will undermine state sovereignty and consumer confidence, while hindering digital transformation and limiting growth.
- Need for multilateral approaches– Multilateral approaches are necessary, and must avoid conflicting legal obligations on service providers.
- Address inefficiencies – Failure to address current inefficiencies and the lack of clarity in the application and understanding of the law will exacerbate the problem of foreign governments bypassing the system by creating data localisation laws.
- Avoid encryption reforms – Regulatory reforms relating to encryption should not require companies to undermine the integrity and security of products and services that customers rely on.

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

1. Introduction

The promised benefits and economic growth in Europe provided by digital technologies can only become a reality when customers fully trust the services they use. Customers also have legitimate expectations that if they entrust their data assets to digital service providers, those providers will manage data securely and in the interests of their customers.

Such interests include an understanding whether and how law enforcement authorities can access customers' data in the course of criminal justice investigations that serve wider public safety interests. **Current rules and practices regarding digital evidence have created some uncertainty among customers, providers, and law enforcement authorities**. In some cases, the uncertainty has led to mandatory localisation requirements, which hinders the potential for innovation that digital services offer. This lack of clarity needs to be resolved in order to enable the economic growth that Europe desires from the overall digital transformation of industry.

Several initiatives are underway in national, EU, and international fora to achieve better clarity, improve efficiency, and resolve conflicts. To contribute to these discussions, this paper updates and expands on DIGITALEUROPE's positions stated in the 2014 paper "Law Enforcement Access to Data in the European Cloud"[1], and more recent press releases following the JHA Council Conclusions on Improving Criminal Justice in Cyberspace (June 2016)[2] and following the Appeals Court decision in the case Microsoft vs the United States (July 2016)[3].

2. Customer requirements, law enforcement requirements, and company obligations

Customers need to know how their data is being managed and expect that access to their data is only possible when clearly authorised. Law enforcement authorities at times seek access to customer data to gather evidence in criminal investigations, and must have clear authority to do so. Society expects law enforcement to be able to investigate crime and gather evidence, while also expecting that such police powers are permitted in defined circumstances subject to safeguards and the rule of law.

DIGITALEUROPE member companies take very seriously their obligation to work with law enforcement, as well as their obligation to protect customer data from any unauthorised access. Maintaining the trust of our users by protecting their privacy and guarding against unreasonable government intrusions is fundamental to DIGITALEUROPE member companies.

Governments around the world have long had the authority to obtain documents or digital records belonging to citizens for evidence in law enforcement investigations. To do so, law enforcement officers must follow legal processes by obtaining the records from the owner who possesses them. The advent of innovative digital services entails two significant changes that have an impact on law enforcement searches and seizures of stored files and data:

- Digitised records are entrusted by owners to service providers, and at times law enforcement authorities' attempt to obtain the data from the providers instead of from the owner of the data directly. Customers

[1] DIGITALEUROPE Position Paper – Law Enforcement Access to Data in the European Cloud (14 Nov 2014)
[2] Joint Statement – Industry supportive of Member States' efforts to improve criminal justice in cyberspace (10 Jun 2016)
[3] PRESS RELEASE – DIGITALEUROPE's reaction to the Decision of the US Court of Appeals in the case Microsoft vs United States of America (15 Jun 2016)

do not expect that they should lose legal protections simply because they move their data from their own offices to a digital service provider.

- Data is often stored by digital service providers in different jurisdictions. Law enforcement investigations seeking physical evidence in another jurisdiction involves established procedures under Mutual Legal Assistance Treaties (MLATs), but experience with such procedures for digital evidence can be cumbersome for law enforcement authorities, who often instead seek to assert extraterritorial jurisdiction over data wherever it might be beyond their borders.

- Law enforcement authorities need to distinguish between the type of data and the nature of the request. Whilst access to content data must be based on a MLAT request (especially for US based services providers), service providers are often able to provide subscriber or metadata directly, if there is a legal basis both in the domestic law of the law enforcement authority as well as in the jurisdiction in which the service provider controlling the requested data is established. Furthermore, in cases of emergency (i.e. where an individual's life/safety are at risk or the security of a State or critical infrastructure) then services providers have procedures in place to provide content directly. Often due to the chain of evidence considerations grounded in domestic law, law enforcement authorities do not wish to receive content data directly in this manner.

Internet service providers handle law enforcement requests and are obliged to cooperate where they fall under jurisdictional authority of a law enforcement agency, yet they also have obligations to their customers to protect their data from unauthorised seizures. Law enforcement efforts to gather evidence directly from service providers create legitimate questions about authority for such searches. For customers deciding whether to utilise the services, uncertainty about such questions can cause them to continue to use less efficient technologies. Such decisions also have an impact on economic competitiveness and growth.

3. Law Enforcement Procedures and Rule of Law

We understand that governments have a need for legitimate access to user data in confronting crime and in strengthening national security, and we support these public safety objectives. A clear acceptance of a rule of law, that authorises data access only in defined and limited circumstances, subject to proper safeguards, is the best way to enhance trust, enable law enforcement activity, and at the same time preserve the interests in privacy and confidentiality.

To achieve the necessary balance of interests and to adjust laws to the digital age, governments should follow a proportional, clear, transparent and periodically reviewed legal framework when they need to access personal data. They should clarify under what circumstances and how they access people's content data, ensuring that any action is properly authorised by a court or a judge and is limited to what is absolutely necessary to achieve a legitimate purpose. Such processes should be transparent, agreed through democratic procedures, and clear for citizens.

Even when laws at the national level provide appropriate safeguards for law enforcement activities domestically, complications and lack of harmonisation hinder cross-border investigations among EU Member States and internationally. Differences between national laws can create conflicting obligations for service providers, and confusion for customers regarding which law governs their data. Within the EU, implementation of the European Investigative Order will assist, but not alleviate the problems of digital evidence gathering. MLATs exist but do not provide a full and adequate international solution.

MLATs were not designed for the digital age, but, in the absence of updated rules, remain relevant because they provide clear and agreed upon procedures. As previously mentioned, while MLATs are not the only avenue for law enforcement agencies to issue data requests, MLATs provide customers and governments with the assurance that laws in their own countries are respected; and companies can provide assurances to governments and to customers that they are not subject to action by law enforcement authorities in another country without respective checks and balances and authorisation by a court or judge of the country that receives the request and where the data is stored. Such safeguards remain needed in any legal reform efforts.

Customers and companies currently expect that governments will use procedures agreed in MLATs where they apply. The EU's General Data Protection Regulation (GDPR) reiterates this understanding in Article 48, relating to limits on international transfers of data demanded by other countries:

> "*Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State*"

If MLAT procedures do not function as efficiently as is necessary to protect public safety, respect for the national sovereignty requires that such procedures be improved and more resources dedicated. The result will not only be more respect for national laws and a greater degree of confidence in cross-border digital services, but also improved coordination in cross-border criminal investigations or other government requests for data access in a third country.

On the other hand, **when governments attempt to hasten their investigations by seeking to obtain evidence stored outside their borders through unilateral demands to service providers, authority for such seizures is doubted and trust in the rule of law is eroded**. The July 2016 appeals court decision in the *Microsoft vs United States* case[4] is significant because the court clarified that the US government does not have authority to exercise its police powers to seize data extraterritorially. This provides reassurance to European customers who expect European law to define the limits and safeguards on law enforcement access. At the same time, the court decision highlights the problems of cross-border investigations and underscores the need to find solutions.

While the rule of law requires a more coherent framework, **we caution against any rules to determine jurisdiction for a Member State to address requests directly to the local office of a company, legally established in another Member State, simply because it has a presence in that Member State**. Many service providers have achieved efficiency by having dedicated teams in place typically in their main establishment in one Member State for handling all law enforcement requests. Through ongoing contacts and the publication of procedures documents, law enforcement authorities know how to address requests directly thereby removing delay and inefficiency by addressing requests to local offices, which in many cases simply act as a post box passing on such requests to central teams who are duly authorised to handle such requests. In particular, law enforcement must not threaten the arrest of local company representatives as a means to compel compliance to orders to seize data that the country is not entitled to seize. A more sensible approach is needed, such as referring to international agreements, including the Budapest convention on cybercrime that provides guidelines on jurisdictional issues.

4 In re: Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp, 2nd U.S. Circuit Court of Appeals, No. 14-2985

In addition, there is a growing debate around law enforcement access to data that is encrypted. Customers (including government customers) have legitimate needs for encryption technology. **We call on the EU to avoid any proposals that would require companies to deliberately undermine the integrity and security of their products, infrastructure and services.** We also urge Member States to strongly endorse innovation in security technologies to ensure that individuals and enterprises can reap the greatest benefits of the digital economy which is central to job creation and economic prosperity in the EU.

4. JHA Council Conclusions on Improving Criminal Justice in Cyberspace

The European Institutions identified the issues relating to the gathering of digital evidence in the European Commission's Communications relating to the Agenda on Security in April 2015[5] and 2016[6], followed by the June 2016 Justice and Home Affairs (JHA) Council Conclusions on Improving Criminal Justice in Cyberspace[7]. The Council Conclusions requested further efforts by the European Commission and proposals by June 2017. **DIGITALEUROPE encourages these efforts and also highlights the role that industry, customer and civil society interests must play in this dialogue.**

The JHA Council Conclusions recommend: (1) enhancing operational cooperation between Member States and the private sector, (2) streamlining MLAT procedures, and (3) reviewing the rules on enforcement jurisdiction in cyberspace, "to explore possibilities for a common EU approach on enforcement jurisdiction in cyberspace in situations where existing frameworks are not sufficient."

The recommendations for review outlined in the Council Conclusions are timely. DIGITALEUROPE member companies intend to participate in the ongoing policy dialogue, keeping in mind their obligations to customers, their legal obligations in multiple countries, and their commitments to human rights standards and to privacy.

The review of law enforcement jurisdiction will be especially important in setting the stage for long term reform. Foremost, we seek solutions that lead towards a more coherent international legal framework that is clear and acceptable to multiple stakeholders.

5 2015 Communication on the European Agenda on Security (28/4/2015), "Section 3.3 Fighting Cybercrime…. Actions include: 'Reviewing obstacles to criminal investigations on cybercrime, notably on issues of competent jurisdiction and rules on access to evidence and information' " (p.20)

6 2016 Communication "Delivering on the European Agenda on Security" (20/4/2016): "A key element in successfully preventing, investigating and prosecuting serious and organised crime and terrorism-related offences is rapidly securing and obtaining digital evidence…. Relevant information is frequently held by private companies, on their servers, often located outside the territory of the investigating law enforcement agency and therefore outside its jurisdiction. Aside from mutual legal assistance procedures and a few limited rules in international agreements, no harmonised approach exists on how to access such information. As a result, a wide array of different national approaches has evolved, which poses problems for investigation. The Commission will engage with the private sector to facilitate cooperation based on a common understanding across the EU on access to electronic information and evidence, and propose solutions, including a legal instrument if required." (pp.8-9)

7 www.consilium.europa.eu/en/meetings/jha/2016/06/cyberspace--en_pdf

5. Moving forward

DIGITALEUROPE endorses near-term efforts to improve criminal justice efforts and long-term efforts to clarify rules relating to law enforcement access to stored data. We are encouraged by the European Commission's review of law enforcement jurisdiction in the EU and are concerned when governments apply their data access laws with extraterritorial reach. **We think the preferred route is through multilateral agreements that establish clear agreed-upon "rules of the road" for obtaining digital evidence across borders that respect privacy, ensure law enforcement swift access to the evidence it needs, and that respect national sovereignty.**

DIGITALEUROPE looks forward to working with the European Institutions on this important issue.

--

For more information, please contact:
Damir Filipovic, DIGITALEUROPE's Director (Digital Enterprise & Consumer 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 62 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, Ingram Micro, 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 IT Corporation, Sharp Electronics, Siemens, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies, ZTE Corporation.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Cyprus: CITEA
Denmark: DI Digital, IT-BRANCHEN
Estonia: ITL
Finland: FFTI
France: AFNUM, Force Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: ICT 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