DIGITALEUROPE

Law Enforcement Access to Data in the European Cloud

DIGITALEUROPE represents the digital technology industry in 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.

Such benefits, and economic growth in Europe, can derive from widespread adoption of cloud computing technology, as recognized in the European Commission's EU Cloud Computing Strategy. However, Europeans may be hesitant to embrace cloud services because of lack of clarity about how their data stored in data centres in different countries might be accessed by law enforcement authorities. The multijurisdictional dimension of cloud computing presents a number of legal challenges.

This paper addresses one of the specific concerns - the extraterritorial reach of law enforcement authorities to access data in the context of routine criminal investigations. We believe that this concern can be effectively corrected by a multilateral dialogue that will enhance the public's trust while also increasing the effectiveness of law enforcement.

A recent US court case[1] has highlighted an approach taken by US law enforcement authorities towards access to personal data stored in European data centres. In this specific case, a US district court judge in New York has upheld a warrant requiring a global cloud provider to deliver a customer's email content, stored in Ireland, to US prosecutors for a criminal investigation. The court held that location of the data was not a relevant factor in deciding whether it had authority to order seizure of the data, and did not require the criminal prosecutors to seek cooperation of Irish authorities, pursuant to the Ireland-US or EU-US Mutual Legal Assistance Treaties (MLATs), in order to obtain the data.

The case raises concerns about how to balance the needs of law enforcement in an Internet-connected world with the sovereignty of individual nations. To the extent the EU has insights and a point of view on these issues, we encourage the EU to consider filing an amicus brief with the appellate court, utilizing the procedure created under U.S. law to ensure that courts have the benefit of this type of information before making a decision. In addition, we urge the EU to call for a multilateral dialogue with the aim of:

1 In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, 13 MJ 2814, US District Court, Southern District of New York.

DIGITALEUROPE
Rue de la Science, 14 B-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) encouraging governments to respect sovereign boundaries, and, therefore, to use MLATs when seeking evidence stored in another country in furtherance of routine criminal investigations in non-exigent circumstances[2]; and 2) calling for further investment in the development of MLAT processes so that they function effectively, which will increase the effectiveness of law enforcement, and obviate the need for cross-border demands directly to providers. To the extent that MLAT procedures are not being used and there is any gap in their scope with regard to digital evidence, we believe that this needs to be addressed.

Maintaining the trust of our users by protecting their privacy and guarding against unreasonable government intrusions is fundamental to the companies. We understand that governments have a need for legitimate access to user data in confronting crime and in strengthening national security, but a better balance must be struck that allows governments to address criminal threats while at the same time preserving the right to privacy.

To achieve this balance, 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 personal data, ensuring that any action ends up being authorized by a court or a judge from the country where user data is located, and is limited to what is absolutely necessary to achieve a legitimate purpose.

Governments around the world have long had the authority to obtain data about citizens for law enforcement purposes. Companies are obliged to cooperate with law enforcement requests, yet also have an obligation to their customers to protect their data from unwanted or unauthorized intrusion. Governments should also cooperate with each other and avoid conflicts of law with other jurisdictions by recognizing that international companies are subject to the local laws wherever they operate.

MLATs between Ireland and the US, and between the EU and the US, establish procedures of cooperation for law enforcement authorities that the Court should have been considered. By using clear and agreed procedures, law enforcement authorities can obtain evidence they need; customers can be sure 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 authorization by a court or judge of the country that receives the request and where the data is stored.

Customers and companies expect that governments will use procedures agreed in MLATs where they apply, and such practices can help provide a greater degree of confidence in cross-border cloud services. 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, rather than set aside. The result will not only be more respect for national

2 See the EC position expressed in "Restoring Trust in EU-US data flows - Frequently Asked Questions", 27 November 2013: "If U.S. authorities circumvent the Mutual Legal Assistance agreement and access data directly (through companies) for criminal investigations, they expose companies operating on both sides of the Atlantic to significant legal risks. These companies are likely to find themselves in breach of either EU or U.S. law when confronted with such requests: with U.S. law (such as for example, the Patriot Act) if they do not give access to data and with EU law if they give access to data. A solution would be for the U.S. law enforcement authorities to use formal channels, such as the MLA, when they request access to personal data located in the EU and held by private companies"

laws, but also improved coordination in cross-border criminal investigations or other government requests for data access in a third country.

DIGITALEUROPE would like to promote long-term efforts to clarify rules relating to law enforcement access to data stored in data centres. We observe with concern that increasingly around the globe governments are adopting law enforcement access laws with extraterritorial reach. As noted above, we think the preferred route is multilateral agreement on "rules of the road" for obtaining digital content across borders that respect privacy, ensure law enforcement swift access to the evidence it needs, and that respect national sovereignty. Legislation recently introduced in the United States Senate[3], highlights some helpful principles that could perhaps inform this debate[4].

DIGITALEUROPE would again encourage the European Commission to engage more vocally in this debate and to engage in a dialogue about the importance of MLAT procedures and national sovereignty.

3 See The Law Enforcement Access to Data Stored Abroad (LEADS) Act
http://www.hatch.senate.gov/public/index.cfm/releases?ID=8e28c3f9-842b-4d96-83b7-9f71cf40bc07

4 The bill's main principles are: governments should access data stored in their own territory only through appropriate legal process; governments should not unilaterally reach across international borders to access email or other private content; when governments need data in another country, they should use established international legal channels like MLATs; MLAT processes should be made more efficient; In limited circumstances, if a government is going to use domestic processes to reach across its borders, it should confine that power to accessing the content of its own citizens; an international convention on government access should be based on respect for human rights, individual privacy and respect for the laws of other countries.

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 58 corporate members and 36 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

Acer, Alcatel-Lucent, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cassidian, Cisco, Dell, Epson, Ericsson, Fujitsu, Hitachi, Hewlett Packard, Huawei, IBM, Ingram Micro, Intel, iQor, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Mobility, Motorola Solutions, NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, Schneider Electric IT Corporation, Sharp Electronics, Siemens, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, Western Digital, Xerox, ZTE Corporation.

National Trade Associations

Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Cyprus: CITEA
Denmark: DI ITEK, IT-BRANCHEN
Estonia: ITL
Finland: FTTI
France: Force Numérique, SIMAVELEC
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: ICT IRELAND
Italy: ANITEC
Lithuania: INFOBALT
Netherlands: Nederland ICT, FIAR
Norway: IKT NORGE
Poland: KIGEIT, PIIT
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: ECID, TESID, TÜBISAD
Ukraine: IT UKRAINE
United Kingdom: techUK