International Working Group
on Data Protection
in Telecommunications

675.56.11

Working paper on
Standards for data protection and personal privacy in
cross-border data requests for criminal law enforcement purposes

63rd meeting, 9-10 April 2018, Budapest (Hungary)

As data is increasingly exchanged and stored around the world, law enforcement has also become an international undertaking. Law enforcement authorities increasingly seek access to personal data held beyond their national borders in criminal investigations. However, these requests present difficult questions of compliance with national and international data protection and privacy standards.

A traditional arrangement for resolving cross-border data requests in criminal matters – Mutual Legal Assistance Treaties (MLATs) – can provide some protections. MLATs facilitate international coordination by law enforcement agencies and reduce conflict, provide a consistent process with oversight, help ensure that officials use appropriate legal channels to request personal data, and reduce legal risk for companies.[1] However, the MLAT system, as it works now, is said to be overburdened by the increasing frequency and complexity of cross-border data requests. Deciphering and meeting each jurisdiction's unique requirements for authorizing access to data is said to pose a challenge.[2]

[1] *See, e.g.*, Agreement on mutual legal assistance between the European Union and the United States of America, 2003 OJ (L181) 34 (routing requests through "central authorities" for review and including Article 9 "Limitations on use to protect personal and other data").

[2] Gail Kent, *Sharing Investigation-Specific Data with Law Enforcement—An International Approach* 7 (Feb. 14, 2014) (Stanford Public Law Working Paper) ("The Central Authorities' burden is further increased by the variety of standards of request that are received…. few countries have national policies or procedures that ensure requests or responses to MLAT requests meet the necessary legal or administrative standards for the other country, which may include specialist language," referencing U.S. "probable cause" standard as an example.).

Secretariat
Berliner Beauftragte für
Datenschutz und Informationsfreiheit
Friedrichstr. 219
D-10969 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

The Working Group has been initiated
by Data Protection Commissioners
from different countries in order
to improve privacy and data protection
in telecommunications and media

Similarly, offices that handle such requests are frequently under-financed and under-staffed.[3] As a result, there could be substantial delays in processing requests, and a response, once received, may not be adequate. In addition, certain countries and data sources are not subject to any MLAT.

Moreover, even official cross-border transfer mechanisms can be opaque. Not all countries clearly report aggregate statistical information about the MLAT process. Alternate arrangements for transferring such data, like voluntary arrangements between providers and foreign governments, can be subject to varied or unknown standards, do not have force of law, and so provide little assurance of protection for the rights of data subjects.

These challenges in executing cross-border data requests create an incentive for governments to resort to other mechanisms. Several countries have asserted unilateral authority to compel companies to produce data, even though the data is held in another jurisdiction. For example, the United States sought to obtain from Microsoft email content held in Ireland.[4] A U.S. appellate court ruled that U.S. law does not authorize warrants for search and seizure of email content stored on foreign severs; on appeal, the U.S. Supreme Court determined the case was moot after the enactment of the "CLOUD Act" authorizing law enforcement access to data regardless of storage location.[5] However, other authorities have required companies to produce data held outside national borders. At risk of violating the U.S. Stored Communications Act, which restricts the disclosure of communications content, Microsoft's Brazilian subsidiary has been fined and a local employee criminally charged by authorities in Brazil for failing to turn over data stored in the U.S.[6] In 2015, a court in Belgium also fined Yahoo for failing to produce IP addresses related to a criminal investigation.[7] Chinese legal authorities now permit certain remote extraction (copying) of data outside of Mainland China when it is not possible to seize the original storage material.[8]

Current activities

Article 32 of the Council of Europe Convention Cybercrime ("Budapest Convention") provides for certain "trans-border access to stored computer data with consent or when publicly available".[9] On a national level, Article 18 requires parties to empower their authorities to order "a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's

---

[3] *See, e.g.*, U.S. Department of Justice, FY 2019 Budget Request - General Legal Activities, Criminal Division 2 (emphasizing the need for further staff and funding to meet "current and expanding" needs of the Office of International Affairs and MLAT processes).

[4] *United States v. Microsoft Corp.*, 138 S.Ct. 1186 (2018).

[5] Id.

[6] *International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests: Hearing Before the H. Comm. On the Judiciary*, 114th Cong. (2016) (written testimony of President and Chief Legal Officer of Microsoft Brad Smith); *see also* Marco Civil (Law 12965/2014), art. 11, par. 2 (applying Brazilian law to foreign Internet companies which offer services in Brazil or have one employee established in Brazil).

[7] Hof van Cassatie [Cass.] [Court of Cassation], Dec. 1, 2015, Pas. 13.2082 N, No. 7, 485 (Belg.) [English translation available at http://journals.sas.ac.uk/deeslr/article/viewFile/2310/2261].

[8] On the handling of criminal cases to collect and review the provisions of a number of issues to determine the electronic data (promulgated by the Supreme People's Court, Supreme People's Procuratorate, Ministry of Public Security, Sept. 20, 2016), http://www.spp.gov.cn/xwfbh/wsfbt/201609/t20160920_167380_1.shtml.

[9] Convention on Cybercrime, Nov. 23, 2001, Europ. T.S. No. 185, Art. 32, https://rm.coe.int/1680081561.

possession or control." The Council of Europe Cyber Crime Committee (T-CY), which represents the state parties to the Budapest Convention, has identified transborder access to cloud data as a high priority and sees a need for amendment.[10] Therefore, in June 2017 the Committee agreed on terms of reference for preparations of a draft 2nd Additional Protocol to the Budapest Convention on Cybercrime to enhance international cooperation.[11] This shall include provisions on more efficient mutual legal assistance, a clearer framework and safeguards, including data protection requirements, but also codification of existing practices and provisions on direct cooperation with providers in other jurisdictions.

The European Commission issued an informal document for discussion on "Improving cross-border access to electronic evidence in criminal matters"[12] in June 2017 and launched a public consultation on the issue which closed at the end of October 2017. The Commission´s initiative "aims to address obstacles in cross-border access to electronic evidence in criminal investigations",[13] which includes considerations to directly compel service providers established outside the European Union, regardless of potentially applicable existing MLATs or other international agreements. The intention of the Commission is to come forward with a concrete legislative proposal in early 2018.[14]

In a press release and "E-evidence Statement", the Article 29 Working Party has raised "several concerns and reservations on the legislative options considered by the European Commission".[15] The Working Party has also pointed out "the necessity to ensure that the future legislative proposal fully complies, in particular, with the existing EU data protection acquis as well as with EU law and case law in general".[16] In the E-evidence Statement, the Working Party especially points to Article 48 of the European Union´s General Data Protection Regulation, which addresses certain cross-border

---

[10] *See, e.g.*, Cybercrime Convention Committee, *Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime* (2017), https://rm.coe.int/terms-of-reference-for-the-preparation-ofa-draft-2nd-additional-proto/168072362b. *See also*, Cybercrime Convention Committee, *Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY* (2016), https://rm.coe.int/16806a495e (report of the T-CY Cloud Evidence Group).

[11] *See supra*, Cybercrime Convention Committee, *Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime* (2017).

[12] Commission Services, Improving Cross-border Access to Electronic Evidence: Findings from the Expert Process and Suggested Way Forward, (2017), https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf.

[13] European Commission, Inception Impact Assessment (2017), https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3896097_en.

[14] Migration & Home Affairs, *e-evidence*, European Commission, https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en. On April 17, 2018 the European Commission finally proposed a "Regulation on European Production and Preservations Orders for electronic evidence in criminal matters" (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0225) and a "Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings" (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:226:FIN). For more, *see* Press Release, Security Union Commission facilitates access to electronic evidence (Apr. 17, 2018), http://europa.eu/rapid/press-release_IP-18-3343_en.htm.

[15] Press Release, Article 29 Working Party, November 2017 Plenary Meeting (Dec. 5, 2017), http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48748.

[16] *Id*.

"transfers or disclosures not authorized by Union law".[17] The Article states that a third country judgment or decision of an administrative authority "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, a mutual legal assistance treaty [MLAT], in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant" to Chapter V of the GDPR. In that matter, the WP29 recalls that EU data protection law provides that existing international agreements, such as a mutual assistance treaty (MLAT), must – as a general rule - be obeyed when law enforcement authorities in third countries request access or disclosure from EU data controllers.[18] Writing on behalf of the European Union, the European Commission's (EC) amicus brief in the *United States v. Microsoft* case concluded that the GDPR makes MLATs "the preferred option for transfers," while noting that a transfer could proceed if other grounds for transfer apply.[19] The EC brief goes on to discuss the applicability of the derogations for the public interest and the legitimate interests of the controller to the specific case.[20]

In the U.S., the "CLOUD Act" was signed into law in March 2018.[21] The Act amends U.S. law to permit law enforcement to compel disclosure of data stored outside the U.S. (subject to challenge by service providers).[22] The CLOUD Act also empowers the executive branch to enter into agreements for foreign governments' direct access to data stored in the U.S. where federal officials certify that government gives sufficient protection to privacy and civil liberties, a decision unreviewable in court.[23]

Observations and Recommendations of the IWGDPT

As more data crosses borders, current and future legal frameworks must maintain strong data protection standards despite divergent national legal regimes. In particular, increased cross-border criminal law enforcement demands for data will pose new challenges should the requesting country authorize access, copying, interception, or other interference with personal data on a basis below established privacy norms.

The mechanisms for facilitating criminal cross-border data access should preserve data protection and privacy interests while encouraging prompt and adequate processing of legitimate cross-border data requests.

Recalling that

- the 51st Meeting of the IWGDPT in Poland recommended that cloud computing must not lead to a lowering of data protection standards as compared with conventional data processing[24]

[17] Statement, Article 29 Working Party, Data protection and privacy aspects of cross-border access to electronic evidence 9 (Nov. 29, 2017), http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610177.
[18] *Id*.
[19] Brief of the European Commission on Behalf of the European Union as Amicus Curiae in Support of Neither Party at 14, United States v. Microsoft, No. 17-2 (Dec. 13, 2017), https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf.
[20] *Id*. at 15.
[21] Consolidated Appropriations Act, 2018, div. V, Pub. L. No.115-141(2018).
[22] § 103.
[23] § 105.
[24] Working Paper on Cloud Computing - Privacy and data protection issues - "Sopot Memorandum", adopted at the 51st meeting of the Working Group on April 23-24, 2012 in Sopot (Poland), https://www.datenschutz-berlin.de/working-paper.html.

- the 54th Meeting of the IWGDPT in Berlin urged governments to allow and encourage citizens to freely research, create, distribute and use tools for secure communications[25]

- the 57th meeting of the IWGDPT in Seoul encouraged governments to provide for mandatory statistical reporting by public authorities of the use of powers to access personal information held by companies[26]

Reaffirming the importance of instruments of international law that provide for the protection of privacy as a fundamental right, in particular

- Article 12 of the Universal Declaration of Human Rights, stating "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks"

- Article 17 of the International Covenant on Civil and Political Rights, stating [that, within a party's territory and subject to its jurisdiction] "(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation", and "(2) Everyone has the right to the protection of the law against such interference or attacks"

- Article 8 of the European Convention of Human Rights, stating "(1) Everyone has the right to respect for his private and family life, his home and his correspondence", and "(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others"

- Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, stating, respectively, that "Everyone has the right to respect for his or her private and family life, home and communications", and "(1) Everyone has the right to the protection of personal data concerning him or her (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified (3) Compliance with these rules shall be subject to control by an independent authority"

Emphasizing the guarantees of an effective remedy for a rights violation, of a fair hearing before an impartial tribunal, and of legality as set out in Articles 8 through 11 of the Universal Declaration of Human Rights, in Articles 2, 14, and 15 of the International Covenant on Civil and Political Rights, Articles 6, 7, and 13 in the European Convention of Human Rights articles, and in Articles 47 and 49 of the Charter of Fundamental Rights of the European Union.

---

[25] Working Paper on the Human Right to Telecommunications Secrecy, adopted at the 54th meeting of the Working Group on September 2-3, 2013 in Berlin (Germany), https://www.datenschutz-berlin.de/working-paper.html.

[26] Working paper on Transparency Reporting: Promoting accountability when governments access personal data held by companies, adopted at the 57th meeting of the Working Group on April 27-28, 2015 in Seoul (Korea), https://www.datenschutz-berlin.de/working-paper.html.

The 62nd meeting of the International Working Group **recognizes** the risks to an individual's privacy and data protection rights where foreign data requests may circumvent protections in national or international law. The Working Group also **observes** that cross-border data requests, based on a clear legal process, serve important national law enforcement needs.

Recommendations

The Working Group recommends that work be undertaken by governments and international organisations to ensure that criminal law enforcement cross-border data requests accord with international human rights norms for the administration of justice and that the criminal law enforcement cross-border data transfer mechanisms, whether MLAT or any other mechanism, be designed to ensure appropriate data protection safeguards and the protection of privacy and correspondence:

- **Accountability**. The transfer mechanisms should ensure that all actors in the process are appropriately accountable for their actions;

- **Procedural Fairness** (Due Process). The transfer mechanisms should ensure that data subjects are guaranteed their rights of procedural fairness (due process) including both clear and transparent legal standards and procedures for requests;

- **Efficacy**. Efficacy of strong transfer mechanisms should be prioritized to facilitate prompt and regular processing of requests, including through the establishment of mutually understood interpretations of any legal standards and procedures for requests and robust resourcing of transfer mechanisms;

- **Notice and Opportunity to Challenge**. Data subjects should have a right to be given notice and an opportunity to challenge a foreign state's request for access to their personal data;

- **Necessary and Proportionate Determination**. No one should be subjected to a lesser standard of legal process than permitted in applicable international human rights law and data protection and privacy frameworks, including necessity and the proportionality to legitimate aims;

- **Judicial Authorization**. The requests should be subject to judicial authorization and review;

- **Oversight**. There should be appropriate independent oversight of transfer mechanisms;

- **Transparency mechanism**. Formal public reporting of aggregate statistics about requests should be required.[27]

[27] See Working paper of the IWGDPT on Transparency Reporting: Promoting accountability when governments access personal data held by companies, adopted at the 57th meeting of the Working Group on April 27-28, 2015 in Seoul (Korea), https://www.datenschutz-berlin.de/working-paper.html.