Introduction and Critique to the "EC Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters "

35C3 Kongress, Leipzig

What's it all about?

- Proposal of the Commission (COM(2018) 225 final) dated 17. Apr 2018
- The proposed regulation is about access to stored data by law enforcement within the scope of an investigation, so this talk is NOT about mass surveillance or preemptive measures
- It compels service providers "enabling legal or natural persons in one or more member state(s) to use the services listed" to directly cooperate with law enforcement from another member state

Scope of the proposed Regulation

- Service Providers are supposed to provide a full copy of all stored data to law enforcement authorities of an enquiring member state
- Data types considered basically include all stored data, i.e. telephone records, email, transaction data, communication data, cloud storage, etc.
- Authorization and limitations for access to data exclusively follow the law of the requesting member state
- There is no requirement to involve or even inform the authorities of the target member state

Which types of services are covered?

"Examples of Service Providers covered" as presented by the Commission at the COPEN meeting, 29/30.05.2018 include:

- Electronic Communication Services as defined by the EECC
- Information Society Services including "social networks, online market places facilitating transactions, and other hosting service providers"
- Internet Domain Name and other IP Numbering Services including "address providers, domain name registries and registrars and related privacy services"

Examples of Electronic Communication Services

Internet access services

BT, Vodafone, NetCologne, Orange, Proximus, Telia, TMobile, Ziggo

Interpersonal communications services

KPN, Vodafone, Tele2, T-Mobile, Simyo, Ben, Hollands Nieuwe, Simpel, Telegram, Skype, WhatsApp, Signal, Messanger, imessage, yahoo, gmail

Conveyance of signals

Anyone who exercises actual control over the transmission of signals over networks regardless of the type of information conveyed (ISPs, satellite network providers, radio and TV broadcasters etc.)

Examples of Information Society Services

Social networks
Facebook, Twitter, LinkedIn, Google+

Online market places
Amazon.com, eBay, Tweedehands.be

Hosting service providers
Amazon Web Services, OVH, cloud service providers for corporate infrastructure

Other information society services that fall within the definition
Youtube, Microsoft Azure, Microsoft Office 365, online gambling website, Itunes

Examples of Internet Domain and IP Numbering Services

IP Address providers
Ripe NCC

Domain name registries
EURid (.eu), SIDN (.nl)

Domain name registrars
OVH.com, SIDN, KPN

Privacy and proxy services
United-Domains AG

Say again…?

- All data stored in a single member state is supposed to be released to a requesting member states LEA within 10 days (or even 6h in case of emergencies)

- The proposal follows the idea that each EU member state is sovereign in its laws and LEA procedures and can follow though with an investigation in all of the EU, regardless of the locality of stored data.

- Service providers are not supposed to check the legality of a request (and will probably not even be able to validate requests from differing regions of law).

- There is, however, no harmonization of criminal law or law enforcement procedures within the EU

Can’t LEAs do this already?

- In principle, LEAs can already request all sorts of stored information to build a case or further an ongoing investigation.

- However, the request will have to be submitted to and processed by the authorities of the seat of the service provider, which will request the information as a proxy.

- Local authorities will only process and forward enquiries which will be punishable under local law and warrant a release of the requested data.

- It is the obligation of the local authorities to observe all local laws, individual and fundamental rights as well as legal remedies concerning the subject in question.

Challenges to Individual Rights

Problem Areas identified (I)

- Enforcement of due process & legal remedies for the individual
- Enforcement of information of the individual (No harmonization within EU!)
- No harmonization on affected legal areas in member states, i.e.
  - abortion in Poland (Email Services)
  - Puigdemont not prosecutable in Germany (Cloud Data)
  - Usage of toll data (Toll Collect)
  - Types of cell data eligible to be requested (Telefonica)
  - Treatment of stored data i.e. personal photos, diaries, company secrets/IP

Problem Areas identified (II)

- A similar measure would never be accepted in the physical world (i.e. a seizure of the Hungarian Police in Austria without information)

- How will differing constitutional rights (i.e. “Kernbereichsschutz” under German Consitutional Law) be resolved? Part of the Lisbon Contract stipulates that data concerning this core of private life protected by §1 Art. 1 GG can not be infringed upon by European Law.

Procedural Problems

Issuing authority (Article 4)

- Every judicial authority of a Member State is authorized to issue a European Production or Preservation Order and contact service providers that offer their services in the EU

- In Germany alone, there are 900 eligible authorities, we estimate 13.000 authorities throughout the EU. It is by no means clear how the authenticity should be established, the service provider will not be able to detect any manipulation

- The problem could possibly be solved were the EU Commission to publish an official list of authorized agencies and orders were to only be electronically transmitted & signed

Regulation of maximum penalties (Article 5) I

- The prerequisite for the issuing of an EPOC or EPOC-PR requires that the specific criminal act is punishable in the issuing state with a custodial sentence of at least 3 years. This stipulation would require an individual examination by the service provider in each case

- A case-by-case examination of this kind is, however, neither affordable, nor is it the task of the provider to check the legality of the state agency's assessment under the proposed regulation

- This will result in service providers of one Member State to be required to produce data, although the offense is not punishable in the (home-) Member State

Regulation of maximum penalties (Article 5) II

- These problems can be solved through a binding, unified list for the European Union, in which specific offenses for which the production of transactional or content data can be requested are recorded in a catalogue

- In parallel to this, the codes of criminal procedures of the Member States must be adapted. Within the scope of the proposed regulation, it must be ensured that companies are not permitted to produce data for foreign authorities that would domestically be subject to a prohibition of the collection or use of evidence.

Relationship to Third Party States

- The law should clearly state that no transfer of data is permitted to Third Party States, be it a member state or otherwise

- This must preclude the possibility that individual Member States negotiate their own agreement with Third States, on the grounds of which certain data can then be forwarded

- The establishment of such an agreement containing mutual obligations should exclusively be possible through the entire Union (i.e. in relation to the US Cloud Act)

Relationship to existing process of voluntary cooperation

- It is unclear if the powers envisaged in E-Evidence with regard to the object of the regulation are to be understood as conclusive
- The EPOC stipulates stricter provisions than some of the existing models of voluntary cooperation of Member States on the basis of prevailing law
- The latter play an essential practical role for the requests to providers from non-EU states for the production of evidence. For the affected providers, it must be clear which constitutional standards apply

Harmonization of the technical provisions

- It is necessary to issue a set of technical guidelines to accompany the regulation in order to implement an efficient and timely response. No specifications are provided for this in the proposal at all (!)

- A broadening of the proposed regulation to include a technical specification is essential in order to guarantee the integrity and security of the data in transit (i.e. like ETSI TS 103 462 for the (similar) EIO)

- Further technical provisions are required to enable the precise, automated identification of the sender and addressee of an EPOC (i.e. in the current proposal an EPOC could be sent even via FAX transmission)

Companies responsibilities

Industry is very critical

- In principle, industry welcomes a unified procedure for a single market
- However, the direct contact of state authorities with individual service providers has first and foremost to do with the discharge of sovereign tasks by the recipient state (no “double tandem”)
- There should be no passing of responsibility to safeguard individual rights from the recipient state to private sector companies
- Many procedural problems with respect to individual rights & companies responsibilities to safeguard user data can be foreseen

Liabilities (I)

- A potential liability of the service provider has not been regulated for in the proposal. It requires clarification that the providers are only acting on an official state order and only carry out measures that have been prescribed by the state

- A passage should be inserted into the law in which the liability of the companies – with the exception of intent and gross negligence – is precluded if the order is refused on legal grounds.

- This should also apply in the case of a manipulation that was not readily detectable for the provider.

Liabilities (II)

- Service providers cannot undertake legal assessments in 28 different legal systems. Given that the liability of the service provider is clearly not intended by the Commission, this should be expressly included and clarified

- Irrespective of this, it must be made clear that there exists a prohibition of the use of evidence for data that has been unjustly collected or produced

- It must be clear that no use of the data is permissible for cases that fall outside of the original grounds for the forwarding of data

Status of the Proposal

Where are we in the Process?

- The proposal for a regulation is **not** passed yet
- Position of the European Data Protection Board, adopted 26. Sep 2018, is very critical
- It was, however, adopted by the Council on 07. Dec 2018
- Parliament held a hearing on 28. Nov 2018, further proceedings are pending. It is unclear if there will be any progress before the EU election in May 2019.

A call to action!

- At the moment, only a handful of countries oppose the regulation (Germany, Netherlands, Finland, Greece, Hungary, Latvia, Czech Republic)
- Advocates for the proposal include France, Spain, Ireland, Belgium, etc.
- We desperately need critical voices in major EU countries, asking their local government as well as MEPs to withdraw support for the proposed regulation
- Talking points - even for the conservative side! - could include the discharge of sovereignty, invalidation of domestic laws and procedures as well as the potential for corporate espionage

Materials used / Recommended reading

EU Proposal for an European Production Order - COM (2018) 225 final
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018PC0225&from=EN>

Opinion of the European Data Protection Board
<https://edpb.europa.eu/sites/edpb/files/files/file1/eevidence_opinion_final_en.pdf>

LIBE Study “An assessment of the Commission’s proposals on electronic evidence”
<http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf>

Thank you for your attention!

Klaus Landefeld
Stellv. Vorstandsvorsitzender
Vorstand Infrastruktur und Netze

eco Verband der Internetwirtschaft e.V.
Französische Strasse 48
10117 Berlin