Legal memo with respect to Law Enforcement Access to Data across Borders - Legal Challenges for Digital Service Providers and Citizen Rights

M. Hans Graux (Timelex Law Offices) and M. Thomas J. Smedinghoff (Locke Lord LLP)

Executive summary

This legal memo investigates the challenges for private sector service providers of complying with recent initiatives that facilitate cross border law enforcement access to data across borders, with a particular emphasis on potential impacts on the European electronic communications and ICT industries.

Specifically, it examines two recent legislative initiatives in greater detail:

1) Firstly, the proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (hereafter the "eEvidence Regulation"). Notably, this memo examines to what extent Europe-based service providers have a right or an obligation to assess the lawfulness of Production and Preservation Orders that target them, and what degree of legal certainty the proposal affords them and European data subjects.

2) Secondly, the recent United States CLOUD Act, including the question to what extent companies in Europe would be able to lawfully comply with US law enforcement requests allowed under this Act, notably in light of conflicting obligations with the General Data Protection Regulation (GDPR) and other European Union data protection laws.

As this memo will argue, these two recent initiatives are likely to create legal uncertainties for EU based service providers in relation to their ability or obligation to comply with law enforcement requests originating from countries other than those in which they are established.

For the former initiative – the eEvidence Regulation – the cause of uncertainty is the fact that service providers' responsibilities and liabilities in the validation of Production and Preservation Orders are not unambiguously defined in the current proposal. Notably, the proposal does not systematically ensure independent judicial review of such Orders by a public authority known to the service provider. As a result, the proposal effectively appears to assign at least some responsibility for ensuring lawfulness of Orders to the service providers themselves, even though they may have neither the resources, nor the information or the legal authority to play this role.

This issue could be resolved by modifying the proposal to ensure that such independent judicial review by public authority known to the service provider (i.e. either within the service provider's

jurisdiction or organised at the EU level) takes place systematically so that the service provider could reasonably assess the formal lawfulness of the request without examining any issues of substance. Alternatively, the proposal could introduce stronger liability exemptions clarifying that the service provider cannot be held responsible or liable for complying with an Order that appeared formally compliant with the terms of the Regulation, explicitly excluding any issues of substance (notably relating to the facts at hand, the legal qualification of these facts, and the competences of the issuing authority), since these are topics which cannot be reasonably assessed by a private sector company.

In relation to the Cloud Act, it seems plausible that EU companies could be targeted by US law enforcement requests provided that a US court would agree that the company has a minimum contact in the US and that the resulting burden on the company satisfies US legal appreciation of fair play and substantial justice. This places such service providers in a legally vulnerable position, since complying with a US request that implies the transfer or disclosure of personal data would require an assessment whether that request is permissible under the GDPR. US law allows for objections against a request to be raised, but will only consider objections based on non-US law (including the GDPR) where an executive agreement exists between the US and the service provider's country. In other cases, only US common law will apply, creating the possibility that the service provider would be liable under US law when not complying with the request, or liable under EU law when complying with it.

The challenges presented by both initiatives underline the importance of organising independent judicial review in cross-border cooperation cases, since private sector service providers cannot reasonably be expected to resolve legal tensions that legislators have been unable or unwilling to address themselves. The creation of legal frameworks that nonetheless require service providers to do so, and that subjects them to liability irrespective of their decisions, is not a sustainable policy.

About the authors

M. Hans Graux is an ICT lawyer and founding partner at the Brussels based law firm Timelex (www.timelex.eu), which specialises in information and technology law in the broadest sense. The team is internationally recognized, being both a Legal 500 Top Tier firm in Information Technology, and a Chambers Europe Recommended Firm for TMT - Information Technology.

M. Thomas J. Smedinghoff is Of Counsel to the Chicago office of Locke Lord LLP (https://www.lockelord.com). He is internationally recognized for his leadership in addressing emerging legal issues regarding electronic transactions, identity management, privacy, information security, and online authentication issues from both a transactional and public policy perspective.

1. The Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters

Context

On 17 April 2018, the European Commission proposed a series of measures to improve cross-border access to electronic evidence for criminal investigations. The measures included a Regulation on European Production and Preservation Orders (hereafter the "eEvidence Regulation") and a Directive on the appointment of legal representatives for the purpose of gathering evidence.

These proposals aim to make it easier and faster for police and judicial authorities to access the electronic evidence they need in investigations. They establish new and more harmonised instruments for direct access to such data across EU borders, as an alternative to the current EU legal framework based on more ad hoc judicial cooperation between authorities of different Member States and with foreign countries. This framework notably includes Directive 2014/41/EU regarding the European Investigation Order in criminal matters (EIO Directive), the Convention on Mutual Assistance in Criminal Matters between EU Member States, and Mutual Legal Assistance Treaties (MLAT) with third countries.

The proposed Regulation introduces binding European Production and Preservation Orders. A European Production Order (EPO) allows a judicial authority in one Member State to obtain e-evidence directly from a service provider in another Member State, which will be obliged to respond within 10 days, and within 6 hours in cases of emergency (compared to up to 120 days for the existing European Investigation Order or an average of 10 months for a Mutual Legal Assistance procedure, according to the European Commission[1]). A European Preservation Order (EPO-PR) on the other hand allows a judicial authority in one Member State to request that a service provider in another Member State preserves specific data, in view of a subsequent request to produce this evidence. In effect, both types of Orders allow judicial authorities in the issuing Member State to "export" their competences to another Member State, provided that the requirements of the proposed Regulation are met.

Both EPOs and EPO-PRs need to be issued or validated by a judicial authority of a Member State, and EPOs can only be issued if a similar measure is available for the same criminal offence in a comparable domestic situation in the issuing State. Both types of Orders can be served directly on providers of electronic communication services, social networks, online marketplaces, other hosting service providers and providers of internet infrastructure, such as IP address and domain name registries. Furthermore, Orders can only target data which is already stored at the time of receipt of the Order; they cannot target future data to be received or require real-time interception of

[1] See https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

telecommunication. If a service provider is not established in the EU but operates in the EU market, it is required to designate a representative in the EU to whom EPOs and EPO-PRs can be served. This ensures that a point of contact for the EPOs and EPO-PRs is available, although it is not guaranteed that the representative or the service provider will be able to respond to the Orders as requested, since national law applying to the service provider may prevent them from disclosing the information to EU authorities. For this specific scenario, Articles 15 and 16 foresee specific review procedures in which conflicts between European Orders and third country law can be resolved. The flipside of this issue (EU providers being targeted by non-EU requests that may not comply with EU law) will be examined in the second section of this memo, on the US Cloud Act.

Both types of Orders can be used only in criminal proceedings, from the initial pre-trial investigative phase until the closure of the proceedings by judgment or other decision. Taking into account the diverging degree of sensitivity of data being targeted, different safeguards for the issuing of Orders are foreseen depending on the type of data being targeted in an Order. The eEvidence proposal foresees four categories of data: subscriber data, access data, transactional data and content data. They are defined as follows:

- *'subscriber data' means any data pertaining to:*
    - *(a) the identity of a subscriber or customer such as the provided name, date of birth, postal or geographic address, billing and payment data, telephone, or email;*
    - *(b) the type of service and its duration including technical data and data identifying related technical measures or interfaces used by or provided to the subscriber or customer, and data related to the validation of the use of service, excluding passwords or other authentication means used in lieu of a password that are provided by a user, or created at the request of a user;*
- *'access data' means data related to the commencement and termination of a user access session to a service, which is strictly necessary for the sole purpose of identifying the user of the service, such as the date and time of use, or the log-in to and log-off from the service, together with the IP address allocated by the internet access service provider to the user of a service, data identifying the interface used and the user ID. This includes electronic communications metadata as defined in point (g) of Article 4(3) of [Regulation concerning the respect for private life and the protection of personal data in electronic communications];*
- *'transactional data' means data related to the provision of a service offered by a service provider that serves to provide context or additional information about such service and is generated or processed by an information system of the service provider, such as the source and destination of a message or another type of interaction, data on the location of the device, date, time, duration, size, route, format, the protocol used and the type of compression, unless such data constitutes access data. This includes electronic communications metadata as defined in point (g) of Article 4(3) of [Regulation concerning the respect for private life and the protection of personal data in electronic communications];*

- *'content data' means any stored data in a digital format such as text, voice, videos, images, and sound other than subscriber, access or transactional data.*

Within the proposal, Orders to produce subscriber and access data can be issued for any criminal offence whilst the Order for producing transactional or content data may only be issued for criminal offences punishable in the issuing State[2] by a custodial sentence of a maximum of at least 3 years, or for specific crimes which are referred to in the proposal and where there is a specific link to electronic tools and offences covered by the Terrorism Directive 2017/541/EU. Furthermore, EPOs for subscriber and access data may also be issued by prosecutors in a Member State, which is not permissible for the other categories of data.

While the Proposal aims to ensure the effectiveness of criminal investigations and provides for certain safeguards which are defined in relation to the sensitivity of the Orders, certain issues are likely to give rise to difficulties in its interpretation and application. This memo briefly examines some of the key issues.

Core concepts – the types of data

As described above, the eEvidence proposal defines four categories of data: subscriber data, access data, transactional data and content data. The distinction is critical for the application of the Regulation, since it determines who may issue an Order, and for which alleged violations it can be issued. It is undoubtedly also for this reason that the requested data category must be specified explicitly both in the EPO and in the EPO-PR.

This categorisation approach is not new to European data protection and privacy policy. It can be found among many other sets of legislation in the General Data Protection Regulation (EU) 2016/679 (defining genetic data and biometric data, and containing specific rules for sensitive categories of processing), the ePrivacy Directive 2002/58/EC as amended (traffic data and location data), the proposed ePrivacy Regulation (electronic communications content and electronic communications metadata), and the repealed Data Retention Directive 2006/24/EC (describing data necessary to trace and identify the source of a communication; data necessary to identify the destination of a communication; data necessary to identify the date, time and duration of a communication; data necessary to identify the type of communication; data necessary to identify users' communication equipment or what purports to be their equipment; and data necessary to identify the location of mobile communication equipment).

[2] It is worth noting that only the punishment in the *issuing* State is taken into account, meaning that it is possible to target a service provider in relation to activities that are not punishable at all, or at least not by a custodial sentence of a maximum of at least 3 years, in the service provider's State of establishment.

The eEvidence Regulation would seek to add a new and separate categorisation which would apply in parallel with other legal frameworks. This can lead to some counterintuitive outcomes; i.e. the term 'content data' in the proposed eEvidence Regulation is not identical to the term 'electronic communications content' in the proposed ePrivacy Regulation, since the latter does not exclude "subscriber, access or transactional data". Inversely, the terms 'access data' and 'transactional data' include but are not limited to 'electronic communications metadata' from the proposed ePrivacy Regulation, which may cause challenges in interpretation and application unless both the eEvidence proposal and the ePrivacy Regulation are approved in tandem in a form that continues to comprise these terms.

Furthermore, it might be counterintuitive to observe that 'electronic communications metadata' was considered to be a single category of data in terms of sensitivity for the proposed ePrivacy Regulation, whereas it can be qualified as either 'access data' or 'transactional data' under the eEvidence Regulation depending on its nature, despite the fact that the eEvidence Regulation considers transactional data to be significantly more sensitive than access data (with the former only being targetable by an Order for criminal offences punishable by a sentence of a maximum of at least 3 years, or for other specific serious crimes).

Beyond the potential challenge of consistency between different legal frameworks, the question can also be raised to what extent the line can be clearly draw between these categories. The European Data Protection Board already noted in its Opinion 23/2018 on the proposal[3] that notably "the definition of "access data" still remains vague, compared to the other categories", and that it had concerns "with regards to the different level of guaranties related to the substantive and procedural conditions for access to the categories of personal data, especially given the practical difficulty to evaluate to which category of data will belong the requested data in some cases. For instance IP addresses could both be classed as transactional data and subscriber data".

The example seems correct enough, especially since Annex I to the proposal includes "type of service, including identifier (phone number, IP address, SIM-card number, MAC address) and associated device(s)" listed as subscriber data eligible for a request; "IP connection records / logs for identification purposes" as access data, and "source IP address, destination IP address(es)" as traffic data. The same applies to log files, which can be either access data, transactional data, or content data according to the Annex – and indeed one might make the observation that, based on the definitions in the proposal, it could also constitute subscriber data since it will often identify the "type of service and its duration including technical data and data identifying related technical measures or interfaces used by or provided to the subscriber". Essentially, the definitions of the proposal mix the nature of the data being requested and its functionality in any given combination; this will inevitably give rise to conflicts of interpretation

Moreover, the proposal is based on a paradigm that appears to have been undercut to some extent in recent years, both in doctrine and jurisprudence, namely that the sensitivity of data can be

[3] Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters (Art. 70.1.b), adopted on 26 September 2018

determined in the abstract depending solely on its nature, and that the degree of protection that should be afforded to the data should therefore depend only on its nature. By way of a clear example, data describing a very unique interface which is only used by an application with a specific and sensitive purpose (e.g. a health care app used by substance addicts) would be hugely sensitive. Despite this fact, it could be qualified as subscriber data in the proposal ("data pertaining to the type of service and its duration including technical data and data identifying related technical measures or interfaces used"), which is afforded only the lowest level of protection. Similarly, access data can indicate already between which persons or companies communications are taking place, which may be sufficient to make inferences on the content of the communication as well (e.g. establishing that communications are taking place between a spouse and a divorce lawyer).

In other words, the broader context of the use of the data, and not only its technical nature, determine the degree of sensitivity. The Court of Justice also ruled as such in its judgement in joined cases C-203/15 and C-698/15 (Tele2 Sverige AB), noting that metadata such as traffic data and location data in the case under consideration (i.e. the indiscriminate and general collection of such metadata for the purposes of fighting serious crime) provided the means of establishing a profile of the individuals concerned, "information that is no less sensitive, having regard to the right to privacy, than the actual content of communications". In other words, an assumption that the nature of the data is a sufficient to determine its sensitivity and the required safeguards – even assuming that the nature of data can be unambiguously determined, which is far from certain – is not a stable basis for the proposal in light of recent court rulings.

A simpler and more homogeneous approach might therefore be preferable. One option might be to reduce the number of categories of data, and to create a risk based case by case assessment mechanism, involving competent authorities rather than the service providers themselves, in a manner that recognises the importance of nuance. This would arguably be more in line with both the risk-based approach of the GDPR, and with recent case law.

On the latter point, reference can also be made to the recent Court of Justice ruling in Case C-207/16 (Ministerio Fiscal), in which judicial authorities requested the production of subscriber data (albeit in a purely national context which would therefore not be subject to the eEvidence Regulation). In this matter, the Court examined a request that would allow specific SIM cards activated within a single stolen mobile telephone to be linked, during a specific period, with the identity of the owners of those SIM cards. Considering that "*Without those data being cross-referenced with the data pertaining to the communications with those SIM cards and the location data, those data do not make it possible to ascertain the date, time, duration and recipients of the communications made with the SIM card or cards in question, nor the locations where those communications took place or the frequency of those communications with specific people during a given period. Those data do not therefore allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned*."

It should be observed that the Court did *not* rule that subscriber data was not sensitive by definition, in the same way that it did not rule that metadata was sensitive by definition in the Tele 2 Sverige AB ruling. Indeed, one might easily imagine a different outcome if the request had targeted all

subscriber information from all persons who had been present in an entire autonomous region over a period of months. It is not the nature of the data alone, but the entirety of the context of use, which determines the scope of the required safeguards.

The critical question is then how those required safeguards can be ensured consistently, and how a risk-based approach could be integrated. This issue will be examined in the following section.

Legal certainty for the addressee during enforcement

In terms of enforcement of an EPO and EPO-PR, it is important to recognise that the proposal already builds in an additional layer of safeguards. The EPO or EPO-PR is not transmitted in its original form by an issuer to an addressee (either a service provider or its representative). Rather, the Order is transmitted to the addressee through a European Production Order Certificate (EPOC) or a European Preservation Order Certificate (EPOC-PR). The EPOC or EPOC-PR by an issuing or validating authority, who signs it and certifies its content as being accurate and correct.

The addressee is expected to act upon the contents of an EPOC or EPOC-PR within the timelines contained in the proposal. However, several exceptions are included where a response is not mandatory. These can be broken down into two major categories:

- Firstly, material impossibility to comply with the Order. Articles 9 and 10 (respectively in relation to and EPOC and EPOC-PR) state several grounds where a response is not possible, including (a) where the EPOC is incomplete, contains manifest errors or does not contain sufficient information to execute the EPOC; (b) cases of force majeure or of de facto impossibility not attributable to the addressee or, if different, the service provider[4]. In these cases, and in situations where the information cannot be provided exhaustively or within the communicated timelines, the proposal foresees a counternotice process that at a minimum suspends response timelines for the addressee.

- Secondly, an addressee may decide that an EPOC or EPOC-PR cannot be executed because based on the sole information contained in the EPOC or EPOC-PR it is apparent that it manifestly violates the Charter of Fundamental Rights of the European Union or that it is manifestly abusive. In other words, this second grounds of refusal requires an appreciation on the substance and contents of the Order, and *only* of the Order, not of its broader context. Here too, there is a counternotice process to the competent enforcement authority in the Member State of the addressee.

If an addressee refuses to respond to an EPOC or EPOC-PR, Article 14 defines a procedure to resolve the issue. The process is relative complex, since it requires the participation of all stakeholders: the

[4] Notably because the person whose data is sought is not their customer, or the data has been deleted before receiving the EPOC or EPOC-PR.

addressee, the issuing authority, and the competent authority in the enforcing State (where the addressee resides). If the issuing authority accepts the response (e.g. because it recognises that the Order was flawed or because there is a material impossibility), no further follow-up is required.

If the issuing authority does not accept the refusal, it can establish a dialogue with the competent authority in the enforcing State of the addressee, providing the Order and the applicable certificates, and any other relevant information required for an assessment by the competent authority. At that point, it is up to the competent authority to determine whether the Order satisfies the requirements of the Regulation. If the enforcing authority recognises the Order, it will formally require the addressee to comply with the relevant obligation, but informing it of the possibility to oppose the enforcement by invoking the grounds listed in the Regulation, as well as the applicable sanctions in case of non-compliance, and set a deadline for compliance or opposition. These ground for opposition are exhaustively listed as follows:

- the EPO or EPO-PR has not been issued or validated by an issuing authority as provided for in Article 4 of the Regulation;
- the EPO has not been issued for an offence provided for by Article 5(4) of the Regulation;
- the addressee could not comply with the EPOC or EPOC-PR because of the material impossibility grounds described above;
- the EPO or EPO-PR does not concern data stored by or on behalf of the service provider at the time of receipt;
- the EPO or EPO-PR targets a service which is not covered by the Regulation;
- based on the sole information contained in the EPOC or EPOC-PR, it is apparent that it manifestly violates the Charter or that it is manifestly abusive.

If the addressee objects under any of the grounds above, the enforcing authority must decide whether to enforce the Order on the basis of the information provided by the addressee and, if necessary, supplementary information obtained from the issuing authority. If the addressee does not comply with its obligations under a recognised Order whose enforceability has been confirmed by the enforcing authority, that authority must impose a pecuniary sanction in accordance with its national law.

While the procedure appears well structured, there are certain underlying assumptions which would benefit from being made explicit. Firstly, the procedure indicates at several points that an addressee *may* refuse a request on the grounds specified in the Regulation. The proposal however does not specify clearly whether the addressee *must* make an assessment. In case of material impossibility, this is of course implicitly included, since providing any response will require an assessment of whether it is possible to respond. But is the addressee *required* to assess whether a request "manifestly violates the Charter of Fundamental Rights of the European Union or that it is manifestly abusive", or is this merely *allowed*?

The same issue applies to the grounds for opposition listed in the Regulation and summarised above, on which basis the addressee *may* oppose the enforcement, while staying mute on whether the addressee is *required* to assess these points and what the consequences of an incorrect assessment would be. This issue is important since it directly determines the incentives for an addressee and impacts the resources it should dedicate to assess and possibly contest Orders.

From a policy perspective, the worst outcome would be an interpretation of the Regulation where an addressee can be held liable for incorrect assessments (including for not opposing a request where this would have been legally possible), since the grounds of objection contain several points on which the addressee is materially unable to make a proper assessment. This includes notably the assessment of whether the Order was issued or validated by an issuing authority as provided for in Article 4, or where the EPO relates to an offence provided for by Article 5(4). Both of these points require an in-depth understanding and knowledge of national law (including national law enforcement and judicial organisation) and of the facts being examine which will simply be unavailable to addressees. Indeed, they cannot and should not be available to addressees: it would not be appropriate for issuing authorities to provide addressees with details of alleged facts and their expected criminal qualifications under national law. None the less, that is precisely the information that addressees would need to be able to assess whether an EPO relates to an offence provided for by Article 5(4).

Clearly, the effect of the Regulation should not be that addressees can be held responsible or liable for decisions that they cannot reasonably make; they must be able to rely on the veracity and legal compliance of the certificates they receive. A minimal possible solution would be to clarify that the addressee is not responsible or liable for verifying compliance with at least these two grounds of objection.

More generally however, the Regulation's approach to the liability of service providers is extremely succinct and subject to harmful interpretations. The proposal mentions summarily in recital (46) that "Notwithstanding their data protection obligations, service providers should not be held liable in Member States for prejudice to their users or third parties exclusively resulting from good faith compliance with an EPOC or an EPOC-PR". While this is a useful statement in its own right, this seems to be a fundamental principle of the Regulation that should be contained in the principal text, and not merely in a recital.

Moreover, it only addresses liability for incorrect decisions made in good faith, but not the more fundamental question of whether an addressee is required to conduct an assessment, and to what lengths it should go. This is a critical point, since it relates to the stewardship over the authenticity of the legality and authenticity of Orders; if the addressees are made responsible on this point, this will create complexities since they simply do not have access to the relevant information for doing so, even leaving aside the more fundamental objection that it may not be advisable from a policy perspective to make private entities the stewards of lawfulness and authenticity of cross border criminal investigative cooperation requests.

An alternative perspective might be to state that service providers have an obligation in principle of trust towards not only their national competent authorities, but also to those in other Member

States, and therefore that they should always comply with requests unless they can demonstrate that one of the grounds of objection stated in the Regulation exist. But this position is also fundamentally flawed, since not all of these grounds of objection can be appreciated by the service providers. Furthermore, it would create an asymmetry, since service providers are able to assess compliance with their national authorities' requests much more easily than for foreign authorities (since at least they can assess the competence of their own authorities and the criminalisation of the alleged facts); obliging them to trust foreign authorities to a greater extent than national ones appears to be an illogical and inefficient outcome from a policy perspective.

More generally, it seems unclear how this issue can be resolved coherently without introducing a central authority at the EU level, or at least within each Member State, who can assess the lawfulness and validity of the EPO and EPO-PR consistently prior to communicating it to the service providers. It should be noted that this position was also taken by the CCBE (the Council of Bars and Law Societies of Europe) in its October 2018 position on the proposal[5].

The CCBE noted that "Some form of judicial review in the executing State would be necessary in order to ensure sufficient protection of fundamental rights. The CCBE therefore suggests that there be used the provisions of Article 11(1) of the EIO Directive 2014/41 on the grounds for non-recognition or non-execution of the order. If it jeopardises the investigations to notify the data subject before the data are handed over, at least a meaningful judicial review must be performed in the executing Member State on the legality of the measure in accordance with the law of that state. Alternatively, consideration could be given to creating a judicial body at European level composed of authorities from all Member States and independent experts (judges and lawyers), which could be required to "greenlight" all orders going to service providers and other entities (similar, for example, to article 15 of the Draft Legal Instrument on Government-led Surveillance and Privacy)".

It might be observed on that point that Article 6 of the proposed Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings already foresees the obligation for Member States to designate a central authority (or more than one central authority), to ensure the application of this Directive in a consistent and proportionate manner; and that these central authorities are subject to a mutual information exchange and assistance obligation. This existing governance model could potentially be expanded to also incorporate the centralised validation approach described above.

Thus, in general, the proposal would benefit from a clarification of the validation mechanisms for EPOs and EPO-PRs, preferably via an independent public authority known to the service provider (i.e. either within the service provider's jurisdiction or organised at the EU level) as also argued via the CCBE, or at the very least through a clarification whether the addressee has any obligation to assess

[5] CCBE position on the Commission proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, 19/10/2018; see https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20181019_CCBE-position-on-Commission-proposal-Regulation-on-European-Production-and-Preservation-Orders-for-e-evidence.pdf

compliance of the Orders with the requirements of the Regulation, taking into account the fact that the addressee will have access only to limited information which will certainly not be sufficient to comprehensively assess compliance.

In addition and in relation to this, the Regulation should be explicit on whether the addressee is liable for its decisions on this point, and precisely for which shortcomings. At a minimum, the proposal should exclude liability in relation to any substantive defects in Orders that cannot be appreciated by the recipient, notably relating to the facts at hand which gave rise to the Order, the legal qualification of these facts, and the competences of the issuing authority, since these are topics which cannot be reasonably assessed by a private sector company. Such exclusion language could conceivably draw upon the example of the liability exemptions for intermediary information society service providers in the e-Commerce Directive 2000/31/EC, which exclude liability when a service provider does not select, modify or otherwise interfere with the information under their charge. In the absence of a clarification on these issues, addressees may instead opt to manage their responsibilities through large scale recourse to the objection procedures to their local enforcing authority, which would undermine much of the anticipated benefits of the Regulation.

2. The CLOUD Act's Enforceability in the European Union

Context

The U.S. enacted the Clarifying Lawful Overseas Use of Data ("CLOUD") Act on March 23, 2018[6]. The CLOUD Act has two main parts. The first clarifies that companies validly served with a subpoena or warrant under 18 U.S.C. § 2703 must produce the information requested regardless of where it is stored[7]. The second directs the establishment of bilateral "executive agreements" to facilitate the sharing of data between the U.S. and other countries[8].

This memo will address two questions regarding the extraterritorial impact of the CLOUD Act:

- Does the CLOUD Act only target U.S. based companies or does it also cover European companies that store information of U.S. citizens/residents in their data servers in the EU?

- In case a request to deliver data stored in the EU is legitimately addressed to a U.S. tech firm, but the firm is a processor that operates on behalf of a European controller – or if the U.S. firm and an EU-based company are joint controllers – to what extent the request can be fulfilled? What is the responsibility of the European controller?

As a threshold matter, we note that our research has turned up no instances in which the U.S. has attempted to serve a subpoena under 18 U.S.C. § 2703 on an entity without a physical presence in the United States. The majority of case law surrounding the CLOUD Act we have found is related to forcing U.S.-based companies to produce information they have stored abroad, not related to companies that are based outside the U.S.

Does the CLOUD Act only target U.S. based companies, or does it also cover European companies that store information of U.S. citizens/residents in their data servers in the EU?

The CLOUD Act amends the Stored Communications Act by adding a provision stating that "*A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within*

[6] Public Law 115-141, §§ 101 through 106

[7] See 18 U.S.C. § 2713

[8] See 18 U.S.C. § 2523

such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."[9]

Basically, along with its other provisions, the CLOUD Act lays out the circumstances under which an electronic communication service or a remote computing service must comply with a U.S. law-enforcement order to disclose data within its "possession, custody, or control," even when that data is "located . . . outside the United States." But although the CLOUD Act expands the geographic scope of the Stored Communications Act, it does not change who is subject to such law enforcement orders or what type of data is covered.

In other words, the objective of the CLOUD Act was to ensure that law enforcement orders to produce data, that are lawfully issued to an electronic communication service or a remote computing service under the Stored Communications Act (e.g., orders seeking the contents of stored communications), would apply to all information in the possession or control of the recipient, regardless of whether such information is located within or outside of the United States. The CLOUD Act was not intended to increase the scope of the persons or entities who could be served with such an order.

Accordingly, determining whether the CLOUD Act applies to European companies requires a determination as to whether the existing Stored Communications Act extends to European companies —i.e., whether such entities are otherwise subject to the jurisdiction of U.S. law. To that end, CLOUD Act § 102(2) notes that one of the Act's purposes is to address problems caused by "*the inability to access data stored outside the United States that is in the custody, control, or possession of communications-service providers that are subject to the jurisdiction of the United States*".

A. The Nature of a 2703 "Warrant"

The Stored Communications Act (like the CLOUD Act) does not contain an express jurisdiction provision. Section 2703 of the Stored Communications Act authorizes the issuance of (1) a subpoena, (2) a court order, or (3) a "warrant" to compel the disclosure of certain electronic data stored by providers of electronic communications and remote computer services[10].

In actuality, a "warrant" under 18 U.S.C. § 2703 is more akin to a civil subpoena rather than a typical criminal search warrant[11]. The use of the term "warrant" has to do with the level of procedural protections afforded the criminal target of the discovery and not with the direction of governmental agents in performing a physical search of premises[12]. Indeed, the "warrant" is served like a traditional subpoena, but requires the government to satisfy more procedural requirements than a

[9] CLOUD Act Section 103(a), adding 18 U.S.C. § 2713 to the Stored Communications Act

[10] 18 U.S.C. §§ 2703(a) and (b

[11] See Matter of Leopold, 327 F. Supp. 3d 1, 11–12 (D.D.C. 2018) (appeal filed September 2018).

[12] Id.; see also Orin S. Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 Geo. Wash. L. Rev. 1208, 1222 (2004)

typical subpoena to issue it. Therefore, an analysis as to when U.S. Courts would have jurisdiction over a foreign corporation to enforce a subpoena is appropriate.

B. In Personam Jurisdiction Over Foreign Corporations

Under U.S. law, there is no "doubt that a U.S. federal court has the power to require the production of documents located in foreign countries if the court has in personam jurisdiction of the person in possession or control of the material."[13] In personam jurisdiction can be based on either physical presence or minimum contacts. "To be sure . . . 'a nation can exercise enforcement jurisdiction only against persons or entities with a presence or assets within its territory.'"[14] However, the Supreme Court has held that the United States may exercise in personam jurisdiction over foreign corporations where such corporations have "sufficient minimum contacts" with the United States[15]. Further, "when in personam jurisdiction is asserted over a nonresident" corporation it must not "offend 'traditional notions of fair play and substantial justice.' [16]" Thus, determining whether the United States may assert personal jurisdiction over a foreign corporation requires a two-step analysis: (1) a determination as to whether the party has established sufficient minimum contacts, and (2) that the assertion of personal jurisdiction is reasonable and comports with fair play and substantial justice[17].

1. Minimum Contacts

The "minimum contacts must have a basis in 'some act by which the [foreign entity] purposefully avails itself of the privilege of conducting activities within the [United States], thus invoking the benefits and protections of its laws.'[…] Jurisdiction is proper . . . where the contacts proximately result from actions by the defendant himself that create a 'substantial connection' with the [United States]." [18]

In determining what contacts are sufficient to satisfy the "minimum contacts" portion of the analysis, courts may consider whether the corporation is designing a product for the U.S. market, advertising in the U.S., establishing channels for providing regular advice to U.S. customers, or marketing to U.S.

---

[13] United States v. First Nat. City Bank, 396 F.2d 897, 901 (2d Cir. 1968) (citing First National City Bank of New York v. Internal Revenue Service etc., 271 F.2d 616 (2d Cir. 1959), cert. denied, 361 U.S. 948 (1960))

[14] In re Search of Info. Associated with [redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc., No. 16-MJ-00757 (BAH), 2017 WL 3445634, at *14 (D.D.C. July 31, 2017) (quoting Jack Goldsmith, Unilateral Regulation of the Internet: A Modest Defence, 11 EUR. J. INT'L L. 135, 139 (2000))

[15] Helicopteros Nacionales de Colombia v. Hall, 466 U.S. 408, 413-414 (1984)

[16] Id. at 414 (quoting International Shoe Co. v. Washington, 326 U.S. 310, 316 (1945)).

[17] See Daimler AG v. Bauman, ——U.S. ——, 134 S.Ct. 746, 762 n.20 (2014). Further, the burden of proving personal jurisdiction is on the party asserting it. See Purdue Research Found. v. Sanofi–Synthelabo, S.A., 338 F.3d 773, 782–783 (7th Cir. 2003).

[18] Asahi Metal Indus. Co. v. Superior Court of California, Solano Cty., 480 U.S. 102, 109 (1987) (quoting Burger King Corp. v. Rudzewicz, 471 U.S. 462, 474 (1985)).

customers through a U.S. distributor[19]. . This analysis is presumably analogous to the "offering goods or services" test that GDPR uses in Article 3(2)(a) to assert jurisdiction over non-resident businesses – or indeed to the eEvidence proposal's definition of 'offering services in the Union' as meaning "(a) enabling legal or natural persons in one or more Member State(s) to use the services [covered by the proposal]; and (b) having a substantial connection to the Member State(s) referred to in point (a)".

In the context of activities over the internet, U.S. courts have looked at the " 'nature and quality of commercial activity that an entity conducts over the internet.' "[20] At the one end of the spectrum, there are situations where a defendant clearly does business over the Internet by entering into contracts with residents of other states which involve the knowing and repeated transmission of computer files over the Internet. In this situation, personal jurisdiction is proper. At the other end of the spectrum, there are situations where a defendant merely establishes a passive website that does nothing more than advertise on the Internet. With passive websites, personal jurisdiction is not appropriate. In the middle of the spectrum, there are situations where a defendant has a website that allows a user to exchange information with a host computer. In this middle ground, the exercise of jurisdiction is determined by the level of interactivity and commercial nature of the exchange of information that occurs on the Website.

2. Fair Play and Substantial Justice

The satisfaction of the minimum contacts portion of the analysis renders personal jurisdiction "presumptively reasonable."[21]. However, a court may not exercise jurisdiction over a foreign corporation where doing so would "offend traditional notions of fair play and substantial justice". Therefore, once the party asserting personal jurisdiction has established sufficient minimum contacts, the party opposing the assertion of personal jurisdiction has the burden of demonstrating that "the presence of some other considerations would render jurisdiction unreasonable."[22]

In determining whether asserting personal jurisdiction over a foreign corporation would offend traditional notions of fair play and substantial justice, courts may consider " 'the burden on the defendant,' 'the forum State's interest in adjudicating the dispute,' 'the plaintiff's interest in obtaining convenient and effective relief,' 'the interstate judicial system's interest in obtaining the most efficient resolution of controversies,' and the 'shared interest of the several States in furthering fundamental substantive social policies.' "[23]

---

[19] Asahi Metal Indus. Co. v. Superior Court of California, Solano Cty., 480 U.S. at 112

[20] Mink v. AAAA Dev. LLC, 190 F.3d 333, 336 (5th Cir. 1999) (quoting Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F.Supp. 1119, 1124 (W.D.Pa. 1997)). Courts have categorized Internet use into "a spectrum of three areas." Id.

[21] Xilinx, Inc. v. Papst Licensing GmbH & Co. KG, 848 F.3d 1346, 1356 (Fed. Cir. 2017)

[22] Burger King Corp. v. Rudzewicz, 471 U.S. at 477.

[23] Burger King Corp. v. Rudzewicz, 471 U.S. at 477 (quoting World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 292 (1980)) (where the Burger King case refers to "states," they may be read to be "nations," Asahi Metal Indus. Co. v. Superior Court of California, Solano Cty., 480 U.S. at 114).

In determining the burden on the party opposing personal jurisdiction, the Supreme Court has considered the geographic distance between the party and the court in the United States, and the burden a non-U.S. corporation will face in having to defend itself in a totally foreign legal system. Further, it has considered whether relevant transactions took place entirely outside of the United States, the effect of extending personal jurisdiction over a foreign corporation on the U.S. Government's foreign relations, and whether other forums are available for resolving any dispute among the parties[24].

Thus, the CLOUD Act may cover European companies that store information of U.S. citizens/residents in their data servers in the EU. But determining whether the CLOUD Act will apply to any particular European company that stores information of U.S. citizens/residents in their data servers in the EU will be based on a case-by-case factual analysis to determine whether in personam jurisdiction is appropriate under U.S. law.

In case a request to deliver data stored in the EU is legitimately addressed to a U.S. tech firm, but the firm is a processor that operates on behalf of a European controller – or if the U.S. firm and an EU-based company are joint controllers – to what extent can the request be fulfilled? What is the responsibility of the European controller?

The CLOUD Act does not distinguish between, or otherwise address, the concepts of data controllers and processors. As noted above, the "subpoena-like" nature of orders under Section 2703 would require an entity with "possession, custody, or control" of the information sought to produce it if the entity is "subject to the jurisdiction of the United States."

Thus, if an EU entity served with a 2703 request for information is a "data controller," it would be obligated to produce the requested information on the ground that it either "possesses" or "controls" the information. And if the information is in the possession of a processor, the controller would still be responsible for ensuring that it is produced, since it "controls" the information.

In the event that an EU entity served with a 2703 request for information is a "data processor," the fact that it is in possession of the information would likely require compliance (notwithstanding any instructions by the controller not to produce the data). Section 2713 requires providers of electronic communication services or remote computing services to comply with their obligations under Section 2703 to disclose information that is in the providers' "possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States." Under the plain language of the statute, it is enough that the information is in the data processor's possession or custody without it necessarily being in the processor's control.

[24] Asahi Metal Indus. Co. v. Superior Court of California, Solano Cty., 480 U.S. at 114.

To the extent a controller or processor believes that EU law prohibits it from complying with a 2703 discovery device, U.S. courts have held that they have the power to compel foreign corporations to produce information even though producing such information would cause the corporation to violate the law of another nation[25]. The CLOUD Act addresses situations in which complying with a 2703 request for information would cause a corporation to violate the laws of another nation only where the U.S. and the other nation have signed an executive agreement[26]. In the absence of an executive agreement, common law international comity analysis applies.

The party resisting the disclosure of information based on foreign law bears the burden of demonstrating that foreign law does, in fact, prohibit disclosure of the information sought. United States v. Vetco Inc., 691 F.2d 1281, 1289 (9th Cir. 1981). In determining whether to compel a foreign a corporation to produce information, even though such production would require it to violate the laws of another nation, e.g., EU law, U.S. courts examine the following factors under principles of common law comity[27]:

> "(1) the importance to the . . . litigation of the documents or other information requested;
>
> (2) the degree of specificity of the request;
>
> (3) whether the information originated in the United States;
>
> (4) the availability of alternative means of securing the information; and
>
> (5) the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the state where the information is located."

Courts have also considered: "the hardship of compliance on the party or witness from whom discovery is sought; and the good faith of the party resisting discovery."[28]

Finally, courts have considered whether the party resisting discovery is a plaintiff, defendant, or non-party to the litigation or action that is the basis for the discovery in the first place[29].

---

[25] Linde v. Arab Bank, PLC, 706 F.3d 92, 109 (2d Cir. 2013).

[26] Public Law 115-141 § 3; codified at 18 U.S.C. § 2703(h)

[27] Société Nationale Industrielle Aérospatiale v. U.S. District Court for the Southern District of Iowa, 482 U.S. 522, 544 n.28 (1987) (quoting Restatement (Third) of the Foreign Relations Law of the United States § 442 (1987))

[28] Wultz v. Bank of China Ltd., 942 F. Supp. 2d 452, 460 (S.D.N.Y. 2013).

[29] See Compagnie Francaise d'Assurance Pour le Commerce Exterieur v. Phillips Petroleum Co., 105 F.R.D. 16, 29, 31 (S.D.N.Y. 1984) (explaining that the Second Circuit refused to enforce discovery actions against foreign corporations non-parties and weighing the fact that the party resisting discovery was the plaintiff)

Thus, while the CLOUD Act also does not address the processor-controller relationship, it requires the production of information in an entity's "possession, custody, or control." Determining whether the CLOUD Act will require production of information in the face of a contravening European Union law will be based on a case-by-case factual analysis to determine such production would comport with notions of international comity under U.S. law.

This can create a complex interaction with the GDPR, since Article 48 (relating to transfers or disclosures not authorised by Union law) governs the recognition and enforceability of 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". The GDPR in such cases only allows the order, which appears to cover requests under the CLOUD Act as well, to be recognised or enforced 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. In the absence of any such international agreement, a transfer of personal data – whether by a controller or by a processor – would likely be construed as unlawful under the GDPR, exposing the service provider to fines.

The Explanatory Memorandum to the proposed eEvidence Regulation very summarily recognises this issue, pointing out that the proposal's provisions on conflict resolution (Articles 15 and 16, addressing cases where European Orders might conflict with foreign law) are "designed to ensure respect both for general blocking statutes, such as for example the U.S. Electronic Communications Privacy Act (ECPA)", and adding that "with the changes brought about by the adoption of the U.S. CLOUD Act, the blocking statute could be lifted if the EU were to conclude an agreement with the US. Additional international agreements with other key partners may further reduce conflicts-of law situations". In other words, the proposal recognises the need for international agreements, but contains no inherent solution mechanism.

The approach taken in the US Cloud Act is in fact very similar, since US law allows for objections against a request to be raised if complying with a request for information would cause a service provider to violate its own laws (thus including the GDPR), but as described above, it would only do so where the U.S. and the other nation have signed an executive agreement to this effect. In other cases, only US common law will be applied by the Court, creating the possibility that the service provider would be liable under US law when not complying with the request, or liable under EU law when complying with it.

In the specific case of a processor subject to the GDPR being targeted by an order under the US Cloud Act, the processor would therefore always be able to argue that it would not be subject to the Cloud Act on the basis of a lack of minimal contact, or on the basis that the application of the Cloud Act would be a violation of the principles of fair play and substantial justice as described above, and the anticipated violation of the GDPR could always be presented as an unreasonable hardship of compliance. Neither of these points is guaranteed to be decisive however, and in the absence of an executive agreement a US Court would not be required to overturn a request for production of personal data under the Cloud Act.

The processor may therefore be in a position where it is compelled to either violate the order under the Cloud Act by electing not to comply with it, which is likely to result in strong sanctions under US law; or to violate both its agreement with the data controller (by engaging in a non-sanctioned and potentially undisclosed transfer) and the GDPR itself, exposing it to both contractual penalties towards the controller and fines under the GDPR.

This issue is unlikely to be conclusively resolved until an appropriate international agreement between the US and EU on this topic (which would also be binding upon the Member States) would be concluded. As noted in a November 2018 Joint EU-U.S. statement following the EU-U.S. Justice and Home Affairs Ministerial Meeting[30], "The United States and the European Union agreed on the importance for both law enforcement and judicial authorities of swift cross-border direct access to electronic evidence, as demonstrated by recent legislation approved or under examination in the United States and the EU. Participants further recognised the benefit of exploring, and agreed to discuss, the possibility of an EU-US agreement to facilitate access to electronic evidence". At this stage however, no such agreement is in place yet.

[30] See https://www.consilium.europa.eu/fi/press/press-releases/2018/11/09/joint-eu-u-s-statement-following-the-eu-u-s-justice-and-home-affairs-ministerial-meeting/