EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Council of Bars and Law Societies of Europe
The voice of the European legal profession

Rue Joseph II, 40/8 - B-1000 Brussels
T.: +32 (0)2 234 65 10 - ccbe@ccbe.eu - www.ccbe.eu

CCBE Assessment of the U.S. CLOUD Act

28/02/2019

The Council of Bars and Law Societies of Europe (CCBE) represents the bars and law societies of 45 countries, and through them more than 1 million European lawyers. The CCBE regularly responds on behalf of its members on policy issues which affect European citizens and lawyers.

In this paper the CCBE sets out its analysis of the United States (US) "Clarifying Lawful Overseas Use of Data Act" (CLOUD Act) and assesses the extent to which its provisions are consistent with European Law.

A. Summary of the CLOUD Act provisions

On 22 March 2018, the Congress of the United States passed the CLOUD Act which amends the United States Code so as to insert new or amended provisions for the accessing by the US government of data stored outside the United States and the accessing by foreign governments stored within the US. The Act was passed, without any real scrutiny, as part of the Appropriations Act 2018, an omnibus measure.

Most important from a European perspective is that the CLOUD Act amends Chapter 121 of title 18 of the United States Code by adding to the Code a new § 2713 with the title "required preservation and disclosure of communications and records."

The addition states that the existing Stored Communications Act ("SCA") also applies to data stored *outside* of the US. The SCA had introduced §§ 2703 et seq. to the United States Code in 1986 with the aim of imposing statutory confidentiality obligations on information providers and to prescribe the circumstances under which the government can compel disclosure of remotely stored electronic communications.[1] The most important SCA provision for a better understanding of the CLOUD ACT is § 2703 United States Code. This provision describes in detail the rules under which a government entity may require disclosure by a provider and the ways by which such communications can be accessed. These are *either* by obtaining a warrant issued in accordance with the Federal Rules of Criminal Procedure (without notice to the subscriber or customer) *or* by using an administrative or grand jury subpoena or a court order (with notice to the affected person), cf. § 2703(b)(1)(A-B). Since notice to the subscriber or customer usually is undesirable, the legal assessment of the CLOUD Act provisions which follows will be based on the assumption that disclosure will normally be requested by means of a warrant.

The immediate impetus for the passing of the Cloud Act was the *Microsoft Warrant* case (*United States v Microsoft, US Supreme Court Case 17-2)* which concerned whether the recovery by the US government of data stored abroad constituted a lawful "domestic search" under the Act as it was possible to recover that data by accessing it from a computer terminal in the United States. The US government contended it did, but Microsoft (who won before the US Circuit Court of Appeals) argued that it did not, and was supported before the US Supreme Court by a number of Amici Curiae (including

[1] cf. S. REP. 99-541, 5, 1986 U.S.C.C.A.N. 3555, 3559.

the CCBE) who also submitted briefs.[2] After the conclusion of oral submissions, and whilst the Court was considering its decision, the Cloud Act was enacted and the US government deserted its appeal, leaving the proper interpretation of the SCA unresolved. Now, the new § 2713 United States Code states:

> "A provider of electronic communication service or remote computing service [i.e. in particular cloud computing] shall comply with the obligation of this chapter [§§ 2703 et seq.] 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 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."

§ 2703 United States Code enables any US governmental entity to issue a warrant in order to require disclosure as set out in § 2713 United States Code. In the event that such a US-based "provider of electronic communication service or remote computing service" receives a warrant, § 2703 provides a legal remedy by which he can seek to have the warrant declared invalid ("quashed") or modified by a US court ("§ 2703 (h) (2) motions to quash or modify").

The provider needs to file the appropriate motion within 14 days after service of the warrant by demonstrating

> "(i) that the customer or subscriber is not a United States person and does not reside in the United States; and
>
> (ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government." (§ 2703 (h) (2) United States Code)

"Qualifying foreign government" is defined as any foreign government that has entered into an executive agreement with the United States, cf. § 2703 (h) (1). The court seized of the issue may grant the provider's request, after having also heard the United States government, if the court finds that:

> "(i) the required disclosure would cause the provider to violate the laws of a qualifying foreign government;
>
> (ii) based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed; and
>
> (iii) the customer or subscriber is not a United States person and does not reside in the United States." (§ 2703 (h) (2) (B) United States Code)

Aspect (ii) requires a "comity analysis" based on eight further criteria which the court needs to take into consideration:

> "(A) the interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure;
>
> (B) the interests of the qualifying foreign government in preventing any prohibited disclosure;
>
> (C) the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider;
>
> (D) the location and nationality of the subscriber or customer whose communications are being sought, if known, and the nature and extent to the United States […];
>
> (E) the nature and extent of the provider's ties to and presence in the United States;
>
> (F) the importance to the investigation of the information required to be disclosed;

[2] Brief of the CCBE as amicus curiae in support of respondent in Microsoft Ireland Case

(G) the likelihood of timely and effective access to the information required to be disclosed through means that would cause less serious negative consequences; and

(H) if the legal process [i.e. the warrant] has been sought on behalf of a foreign authority pursuant to section 3512, the investigative interests of the foreign authority making the request for assistance." (§ 2703 (h) (3) United States Code)

Potential addressees of § 2713 are internet companies such as Google, social networks like Facebook, Instagram, and Twitter, as well as cloud technology providers, domain name registries, registrars and "digital marketplaces" that allow consumers and/or traders to conclude peer-to-peer transactions.[3]

§ 2713 United States Code, at first glance, applies only to companies based in the United States. However, U.S. extraterritorial warrants could apply to foreign companies if there is a sufficient jurisdictional nexus. So the messenger service Telegram, although not US person, could be subject to an order since it serves US customers.[4]

B. Positive changes resulting from the CLOUD Act

The CCBE regards as a positive development the circumstance that governmental access to data stored outside the United States is now based on a legally established framework that also sets out procedures by which service providers might challenge a warrant. This creates a greater degree of legal certainty for service providers than under the previous SCA regime, where providers had to litigate a contempt finding in order not to have to comply with a warrant (as, for example, in the Microsoft warrant case).

Furthermore, the CCBE recognises the incentive (see § 2523 of the United States Code as amended) for foreign governments to enter into executive agreements with the United States on access to data concerning US citizens or permanent residents. On the basis of executive agreements under § 2523 United States Code, service providers are authorised to respond to requests by foreign governments for information, rendering cross-border information requests easier. Although, in principle, welcoming these steps towards formalisation of cross-border processes, the CCBE still harbours major concerns, not least because of the unilateral approach taken by the legislation.

C. General Concerns regarding the CLOUD Act

I. Short legislative procedure

The CLOUD Act had not received a committee hearing in either the House or the Senate. To the CCBE, such a truncated legislative procedure is highly surprising, given that the same legal matter was highly disputed in the *Microsoft case* before the Supreme Court. The Supreme Court had to deal with numerous *amicus curiae* briefs containing strong arguments both for and against the legitimacy of the disclosure order in question[5]. Although the question of need for and manner of a legal assessment of the application has now been dealt with by the CLOUD Act, the factual complexity of such applications has not changed. The CCBE would therefore have wished that the CLOUD Act had undergone a full and in-depth debate.

II. Extraterritorial jurisdiction

The CLOUD Act grants US law enforcement agencies unlimited jurisdiction over any data controlled by a service provider with sufficient connecting factors to the US (see above).

---

3 https://www.eff.org/de/deeplinks/2018/04/us-cloud-act-and-eu-privacy-protection-race-bottom.

4 https://www.eff.org/de/deeplinks/2018/04/us-cloud-act-and-eu-privacy-protection-race-bottom#_ftn1.

5 *Ibid*.

In consequence, well established procedures to permit access to personal data stored outside a nation's jurisdiction such as Mutual Legal Assistance Treaties (MLATs) are ignored and efforts to adapt them to new challenges are undermined. The CCBE considers this to be an unwelcome development and suggests that it would be more appropriate that rules and procedures for access by law enforcement agencies to personal data stored in foreign jurisdictions should be formulated by means of international consensus and agreement.

The European Parliament addressed the matter in its resolution on Cybercrime by expressing "concern regarding extraterritorial reach by law enforcement authorities in accessing data in the context of criminal investigations and underlin[ing] the need to implement strong rules on the matter"[6],

while at the same time calling on the European Commission to counter

> "the assumption of extraterritorial jurisdiction by third countries."

By far more explicit, the European Parliament stated its concern on 5 July 2018, noting that the CLOUD Act

> "expands the abilities of American and foreign law enforcement to target and access people's data across international borders without making use of the mutual legal assistance treaty (MLAT) instruments, which provide for appropriate safeguards and respect the judicial competences of the countries where the information is located"[7]

and considered

> "that a more balanced solution would have been to strengthen the existing international system of MLATs with a view to encouraging international and judicial cooperation; [in particular because], as set out in Article 48 General Data Protection Regulation, mutual legal assistance and other international agreements are the preferred mechanism to enable access to personal data overseas".[8]

Moreover, the Cloud Act creates a dangerous precedent for other countries. It creates a precedent for any country which is so minded to seek to compel the recovery of data stored anywhere in the world based only on that nation's judicial authority. The CCBE expresses its severe reservations with respect to such measures, which have as their effect the unilateral extension of long-arm jurisdiction.

III. Conflicting laws

The Cloud Act is in conflict with basic human rights, since it fails to provide the minimum standards set out by European Courts to restrict electronic surveillance by government. Both the European Court of Human Rights and the European Court of Justice have indicated a strong preference for prior judicial review and a requirement for a sufficient factual basis for any surveillance of an individual.

Moreover, disclosure of personal data stored within the European Union to a US governmental agency based on a CLOUD Act warrant violates the General Data Protection Regulation (GDPR). According to the GDPR provisions, a US warrant does not constitute a legal basis for such a transfer outside the European Union.[9]

---

6 European Parliament resolution of 3 October 2017 on the fight against cybercrime (2017/2068(INI)), art. 63 and 80, available at http://ww.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0366+0+DOC+XML+V0//EN&language=EN.

7 European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield, recital 27 available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0315+0+DOC+PDF+V0//EN

8 European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield, recital 28 available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0315+0+DOC+PDF+V0//EN

9 See Brief of the CCBE as amicus curiae in support of respondent in Microsoft Ireland Case

Fundamental Rights

Art. 8 of the European Convention on Human Rights and articles 7 and 8 of the European Charter of Fundamental Rights recognise a fundamental right to privacy. According to the jurisprudence of the European Court of Human Rights and the European Court of Justice, any interference with the right to privacy must be in accordance with law, for a legitimate purpose and limited to what is necessary in a democratic society.[10] Where data privacy rights are concerned, both courts apply a "strict necessity" standard.[11] Both the European Court of Human Rights (applying the European Convention) and the European Court of Justice (applying the European Charter) have established numerous safeguards for government monitoring of electronic communications.[12]

a) Lack of notices and legal remedies

The CLOUD Act lacks a thorough system for protecting privacy by procedural and organisational standards. No notice is provided on any level. Neither the state where the data is stored nor the state of which the affected person is citizen are given notice. Most importantly, according to the European Court of Human Rights, notice and an effective remedy should be provided to the affected individual because notice is linked to the effectiveness of remedies. In *Szabó*, the European Court of Human Rights held that notification should be made as soon as surveillance measures are terminated and the notification no longer jeopardises the investigations.

With respect to legal remedies, the CLOUD Act likewise undermines article 19 of the Agreement between the United States and the European Union on the Protection of Personal Information in relation to the Prevention, Investigation, Detection and Prosecution of Criminal Offenses (DPPA). Article 19 DPPA establishes an obligation for the Parties to provide, in their domestic law, specific judicial redress rights to each other's citizens.

b) Unclear scope and duration of surveillance measures

The Cloud Act lacks adequate limits with respect to the scope and duration of surveillance measures.

There is no indication as to the circumstances in which public authorities are empowered to resort to the surveillance measures described in the CLOUD Act. The European Court of Human Rights demands a clear definition of both the "nature of the offences which may give rise" to an order and "a definition of the categories of people liable to" to be surveilled.[13] As a minimum safeguard in this respect, the CLOUD Act should specify the nature of the offences in respect of which the CLOUD act is applicable, either by specifying those offences or at least referring to minimum levels of punishment allowed.

The European Court of Human Rights has clarified that this twin requirement does not mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Instead "foreseeability" means the existence of clear, detailed pre-requisites in order to minimize the risk of arbitrary decisions. In the case *Weber v. Germany* (App. No 54934/00) the European Court of Human Rights held a law to be reasonably foreseeable based on the facts that the law stated the exact offences for which surveillance could be ordered and required the target to have made international phone calls using specific technologies or saying specific catchwords ((recital 97 of the judgment stating "the persons concerned had to have taken part in an international telephone conversation via satellite connections or radio relay links (or

---

[10] E.g. European Court of Human Rights, Liberty v. United Kingdom, App. No 58243/00, http://hudoc.echr.coe.int/eng?i=001-87207.

[11] European Court of Human Rights, Szabó, App. No. 37138/14 at 33; European Court of Justice, Digital Rights Ir. Ltd., v. Minister for Commc'ns, Marine & Nat. Res., at 52.

[12] European Court of Human Rights, Zakharov v. Russia, App. No. 47143/06, http://hudoc.echr.coe.int/eng?i=001-159324.

[13] European Court of Human Rights, Zakharov v. Russia, App. No. 47143/06, http://hudoc.echr.coe.int/eng?i=001-159324.

also via fixed telephone lines in the case of monitoring to avert an armed attack on Germany, in accordance with section 3(1), point 1).

Appropriate restrictions on duration include a clear indication of the period after which an interception warrant will expire, the conditions under which a warrant can be renewed and the circumstances in which it must be cancelled. There are no provisions in the CLOUD Act establishing such time limits.

c) Further safeguards

Under the European convention, the legality and necessity of a surveillance regime is further assessed based on the accessibility of the domestic law, the procedures to be followed for storing, accessing, examining, using, communicating and destroying the intercepted data, the authorisation procedures and the arrangements for supervising the implementation of secret surveillance measures.[14]

Most likely, warrants under the CLOUD Act will not meet the European Courts' standard of accessible (meaning publicly available) terms of surveillance. For example, in *Liberty v. United Kingdom*, annual reports in which the UK Secretary of State's simply affirmed without providing further details that "arrangements" ensured restricted access to material collected via surveillance was held not to "contribute towards […] the clarity of the scheme, since the [Secretary of State] was not able to reveal what the 'arrangements' were."[15]

Data obtained by surveillance measure must also not be stored limitless. In principle, data needs to be destroyed immediately if it is no more relevant for the purpose for which it has been obtained.[16] Even if the stored data is relevant, retaining the data for a longer period of time needs to be justified by objective criteria.[17] For example, no data may be retained of "persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime."[18]

GDPR

Warrants issued based on the CLOUD Act are also in conflict with the EU's GDPR. A warrant alone generally does not supply a legal basis for data processing under the GDPR.

Consent may not justify data processing under the CLOUD Act, because the data subject is not given notice of the issue of the warrant. Valid consent, however, requires to be adequately informed and to have the possibility to withdraw consent. These requirements are not met in a law enforcement environment.

Neither does Art. 6 (1)(c) GDPR justify such processing. Although Art. 6 (1)(c) recognises the necessity "for compliance with a legal obligation to which the controller is subject", such legal obligation must arise out of EU law. Consequently, an obligation under the Cloud Act does not constitute a legal obligation in the sense of Art. 6 (1)(c) GDPR.

Art 48 of the GDPR provides

> "Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement such as mutual

[14] European Court of Human Rights, Zakharov v. Russia, App. No. 47143/06, http://hudoc.echr.coe.int/eng?i=001-159324, at 60.

[15] European Court of Human Rights, Liberty v. United Kingdom, App. No 58243/00, http://hudoc.echr.coe.int/eng?i=001-87207.

[16] European Court of Human Rights, Zakharov v. Russia, App. No. 47143/06, http://hudoc.echr.coe.int/eng?i=001-159324, at 64.

[17] European Court of Justice, Digital Rights Ir. Ltd., v. Minister for Commc'ns, Marine & Nat. Res., at 63.

[18] European Court of Justice, Digital Rights Ir. Ltd., v. Minister for Commc'ns, Marine & Nat. Res.

legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter."

Under this provision, only MLATs or comparable international agreements provide a permissible basis for the extraterritorial transfer of personal data. Thus, the CLOUD Act does not constitute a legal basis for transferring data to the United States under art. 48 GDPR. A US warrant does therefore not meet Article 48's requirements for the transfer of data to the United States from Europe.

A data transfer on basis of a CLOUD Act warrant is neither admitted by art. 49 GDPR, because this exemption is narrow and to be interpreted strictly. Most likely, a warrant issued on basis of the CLOUD Act will not meet the restrictions set out by art. 49 (1) GDPR since the addressee of the warrant (i.e. the service provider) will not be able to assess the circumstances of the data transfer because the Government may not be willing to give away information about the surveillance. Besides, the derogation of art. 49 (1)(d) does not apply because the public interest cannot be based on a unilateral decision by a third country.[19]

As addressees of a CLOUD Act warrant, technology companies will find themselves in the middle between conflicting data laws. Given that the GDPR strictly limits the circumstances under which data may be legally transferred to non-EU countries and provides severe fines for violations (mounting up to 4% of a company's turnover), companies are caught between defiance of a U.S. warrant (for violating a CLOUD Act order) and the risk of substantial monetary or even criminal penalties (for violating GDPR provisions). National laws complementing the GDPR provide prison sentences up to three years for GDPR violations (Sec. 42 (1) new German Federal Data Protection Act).

IV. Limited legal remedy for affected service provider

The CCBE welcomes the fact that the CLOUD Act ensures surveillance not to be ordered "haphazardly, irregularly or without due and proper consideration" by making any procedure authorising surveillance subject to prior judicial review.

Although it is positive – compared to the situation prior to the CLOUD Act – that there now is a well-established process for challenging a warrant prior to its enforcement, the legal remedy to do so is of limited scope.

Providers that find themselves in a dilemma in between EU legal obligations and the obligation to comply with the SCA/ CLOUD Act warrant, are once again left to refuse compliance and litigate a contempt finding, because they are not able to file the motion to modify or quash the warrant. This is due to the fact that the EU – as explained above – does not fall under the term "qualified government" because it is a supranational organisation. Thus, the provider is not able to state a "material risk that [he] would violate the laws of [the] qualifying foreign government" by following the warrant. Such reasoning of a material risk, however, is an essential pre-requisite for the motion, as the word "and" in § 2713 United States Code clarifies.

Even if, however, the term "qualifying government" was to be interpreted broadly so as to apply to supranational organisations as the EU, the EU is likely hindered into entering an executive agreement under § 2523 United States Code by art. 48 GDPR (see above). The same applies to the EU Member States themselves, because they are equally bound by art. 48 GDPR. Instead it would be necessary that the United States enter into an international agreement such as a mutual legal assistance treaty with the EU or all of the EU Member States which so far the United States seem unwilling to do.

In consequence, the pre-enforcement judicial control is in fact non-existent for subscribers and customers that are citizen of an EU Member State.

---

[19] See also the European Data Protection Board Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, page 10-11.

A judicial review prior to enforcement of the warrant should be irrespective of whether the State the required information is stored in is a "qualified government" or not. The requirement (ii) for filing a motion referring thereto should therefore be changed into: "(ii) that the required disclosure would create a material risk that the provider would violate the laws of the foreign state where the requested information is located."

V. Weak (judicial) review

As explained before, the EU would violate its own laws, namely art. 48 GDPR, by entering into an executive agreement under § 2523 United States Code. Even if the EU, however, would enter into such an agreement to have its interests recognised in the prior judicial review following a motion, the comity criteria show shortcomings.

First, the "qualified foreign government" is – other than the US government – not being heard prior to the comity analysis. It is therefore likely that the competent court will accord more weight to the interests of the United States than to the interests of the "qualified foreign government" against disclosure.

Secondly, since the nature and severity of the offences in question are no pre-requisite for issue of the warrant, they should at least be a criterion to be considered in the comity analysis.

Thirdly, criterion (F) relating to the importance of the information to the investigation is construed too broad. Instead, § 2713 should state that a disclosure is only allowed in case the investigation would be disproportionately more difficult or offer no prospect of success.

Lastly, a general prior judicial review would be desirable. With regard to the comity analysis, the CLOUD Act should be changed from "(i) the required disclosure would cause the provider to violate the laws of qualifying government; […]" to "(i) the required disclosure would cause the provider to violate the laws of the state where the requested information is located". Likewise, the specifications (A) to (H) with such reference should be amended.

VI. Lack of post-authorisation supervision

The CLOUD Act makes no provision for any post-authorisation supervision. Yet, such supervision arrangements are a vital safeguard. In *Schrems v Data Protection Commissioner,* the European Court of Justice held that a national supervisory authority has to "examine, with complete independence, any claim concerning the protection of a person's rights and freedoms in regard to the processing of personal data". Such post-authorisation supervision could take the form of a requirement for an annual report on the measures ordered pursuant to the SCA/ CLOUD Act to be submitted to a committee of the House. The report could be required to indicate the number of proceedings brought and the underlying criminal offences to which those proceedings related. In order to guarantee transparency, the Report should be required to be published.

D. Lack of protection of legal professional privilege and professional secrecy

I. Legal professional privilege/ professional secrecy in general

The CCBE is especially concerned that the CLOUD Act does not take into account the particular sensitivity of confidential communications between lawyers and their clients. All professional associations of lawyers in all EU Member States view secrecy as being inherent in the very profession

of lawyers. It is mentioned in all national codes of conduct, following the example of the CCBE.[20] Confidentiality is part of the ethics of the lawyer's profession.[21]

Although European states take different approaches toward protecting professional secrecy and legal privilege, the principle of such protection is generally recognised. Throughout the EU Member States, (and Member States of the Council of Europe) it has the rank of a fundamental principle and the status of a rule of public policy.[22]

In article 41 of the European Charter of Fundamental Rights, the protection of professional secrecy is expressly stated, enshrining

> "the right of every person to have access to his or her file, while respecting the legitimate interests of confidentiality and of professional and business secrecy".

The recognition of legal privilege and professional secrecy before European courts has a long history, in individual jurisdictions pre-dating both the EU and the Council of Europe. Through its case-law, the European Court of Justice has upheld the principle of the confidentiality of written communications between a lawyer and his client,[23] and recognised the specific nature of the legal profession.[24]

The European Court of Human Rights requires all signatories of the European Convention to ensure the sanctity of legal professional privilege or professional secrecy within their territory. In *Michaud v. France*, the Court stressed that the exchange between lawyers and their clients enjoyed strengthened protection. The European Court of Human Rights' case law reveals two different principles in which the protection of legal privilege and professional secrecy has its roots. In its judgement in *Niemitz v. Germany*, the Court ruled that where a lawyer was involved, an encroachment on professional secrecy "may have repercussions on the proper administration of justice and hence on the rights guaranteed by Article 6 [the right to a fair trial]."[25] Without the certainty of secrecy, there is no confidence in the relation between client and lawyer. In effect, there is no basis that could lead to the "manifestation of truth and justice"[26]. Likewise, Advocate General Léger stated in his opinion in *Wouters and Others* that "lawyers occupy a central position in the administration of justice as intermediaries between the public and the courts."[27] Legal privilege thus is the essential corollary to the client's right of defence.[28] The second aspect of legal privilege and professional secrecy is that the principle protects citizens from disclosures with the potential to damage their reputations. With regard to this protecting purpose, the European Court of Human Rights held in its judgment *Foxley v. the United Kingdom*, that the right to privacy under art. 8 of the European Charter of Human Rights is another essential component of the principle.[29]

In summary, the protection of legal professional privilege is now seen to derive from article 8 (1) (protection of correspondence) in conjunction with article 6 (1), (3)(c) of the European Charter of Human Rights as well as from article 7 of the Charter of Fundamental Rights of the European Union

---

[20] Opinion of Advocate General Poiares Maduro in Case C-305/05 before the European Court of Justice, delivered on 14 December 2006, recital 37.

[21] Opinion of Advocate General Poiares Maduro in Case C-305/05 before the European Court of Justice, delivered on 14 December 2006, recital 37.

[22] See, to that effect, recital 182 of the Opinion of Advocate General Léger in European Court of Justice, Case C-309/99, Wouters and Others.

[23] European Court of Justice, Case 155/79 AM & S [1982], ECR 1575.

[24] European Court of Justice, Case C-309/99, Wouters and Others [2002] ECR 1-1577.

[25] European Court of Human Rights, judgement of 16 December 1992, Niemitz v Germany, § 37.

[26] Opinion of Advocate General Poiares Maduro in Case C-305/05 before the European Court of Justice, delivered on 14 December 2006, recital 41.

[27] Opinion of Advocate General Léger in European Court of Justice, Case C-309/99, Wouters and Others, recital 174.

[28] European Court of Justice, case 155/79, AM & S v Commission [1982] ECR 1575, recital 10 and 23.

[29] European Court of Human Rights, judgment of 10 September 2000, *Foxley v the United Kingdom*, § 44.

(respect for communications) in conjunction with article 47 (1), the second sentence of article 47 (2) and article 48 (2) of that Charter (right to be advised, defended and represented, respect for rights of the defence).[30]

II. Lack of procedural protections

The CLOUD Act threatens to compromise the inviolability of legal advice without providing lawyers or their clients with any procedural protections to secure the privilege granted by EU law.

The European lawyer's right to protection of legal privilege and professional secrecy with respect to the seizure of potentially privileged material held on data servers throughout Europe is not addressed in the CLOUD Act and SCA respectively. A broad and undifferentiated seizure of email correspondence, however, was held to violate the principle of legal privilege and professional secrecy by the European Court of Human Rights.[31]

Likewise, Advocate General Kokott stated in *Akzo and Akcros v Commission* that

> "[l]awyers would be unable to carry out satisfactorily their task of advising, defending and representing their clients, who would in consequence be deprived of the rights conferred on them by Article 6 of the European Charter of Human Rights and by Articles 47 and 48 of the Charter of Fundamental Rights, if lawyers were obliged, in the context of judicial proceedings or the preparation for such proceedings, to cooperate with the authorities by passing them information obtained in the course of related legal consultations."[32]

This applies all the more so when lawyers do not even have any knowledge of the seizure of protected material, because the disclosure procedure on basis of a warrant does not involve any notice. As long as the CLOUD Act does not provide for the inadmissibility of evidence gained from protected material, the CLOUD Act threatens to deprive European citizens of their rights to privacy, representation and a fair trial.

The ECHR article 6 right to a fair trial is absolute (unlike the article 8 right to privacy, which is qualified) and for that reason, the CCBE suggests that the existence of legal professional privilege or professional secrecy in the data sought to be recovered should be an absolute bar to the recovery of such data. In this regard, it should be noted that material protected by legal professional privilege and professional secrecy might, in some circumstances, be found in communications data as well as content data. At the very least, legal professional privilege and professional secrecy of lawyers should be listed as a factor to be taken into account in the "totality of the circumstances" as part of the comity analysis. If this is not done, legal professional privilege and professional secrecy is likely not to be taken into account at all. Although the United States recognises an "attorney-client privilege" as an absolute rule of evidence the effect of which is that defendants in a criminal case are not compelled to produce to the prosecutor any "reports, memoranda, or other documents made by the defendant, or the defendant's attorney or agent, during the case's investigation or defense" (Federal Rule of Criminal Procedure 16(b)(2)), enforcing this principle is difficult throughout the non-adversarial collection of evidence.

Adding legal professional privilege and professional secrecy as a weighing factor to a (general) comity analysis is even more important, given that there is no post-seizure judicial control.

Furthermore, professional secrecy obligations in some European nations may be of broader scope than in the United States: Under the Belgian Judicial Code, for example, communication between lawyer

---

[30] Opinion of Advocate General Kokott in European Court of Justice, Case C-5550/07, delivered on 29 April 2010, Akzo Nobel Chemicals and Akcros Chemicals v Commission, recital 47.

[31] European Court of Human Rights, Vinci Construction and GTM Génie Civil et Services v. France, App. Nos 63629/10 and 60567/10, 2 April 2015.

[32] Opinion of Advocate General Kokott in European Court of Justice, Case C-5550/07, delivered on 29 April 2010, Akzo Nobel Chemicals and Akcros Chemicals v Commission, recital 49 with further reference.

and client may not be used as evidence and any privilege dispute must be resolved by the head of the Belgian bar association.[33] Any disclosure process based on a CLOUD Act warrant would therefore run contrary to Belgian law.

E. Impact on the Privacy Shield

In theory, the CLOUD Act leaves the Privacy Shield unaffected, because the latter applies to transatlantic data transfer between private entities for commercial purposes, whereas the CLOUD Act applies to transatlantic data transfer from a private entity to a governmental agency for law enforcement and prosecution purposes. In practice, however, the CLOUD Act does nothing to address the risk that, after a transatlantic transfer for commercial purposes, personal data will be made the subject of a requirement of a disclosure obligation for prosecution purposes. The doubts as to how much protection the Privacy Shield actually provides, which was in particular raised in connection with the Microsoft case, therefore remain.

However, it might be unlikely that the Commission, due to the CLOUD Act, changes its adequacy assessment of the Privacy Shield. Prior to the passing of the CLOUD Act, the US government was able to access personal data of an EU citizen – transferred to the US in compliance with the Privacy Shield and then stored within the US – on the basis of the SCA. Although the SCA did not provide any legal remedies, the Commission came to the conclusion that the US ensures an adequate level of data protection. A by far more realistic assessment of the data protection level would have been to judge online-based US service providers as being insecure and not compliant with GDPR provisions, because there is a risk of unrestricted processing by US authorities subsequent to an SCA warrant. As this risk remains, the conclusions of the Commission as to the adequacy of the Privacy Shield remain in this respect, questionable and still need to be challenged.

F. Recommendations

In order to eliminate the conflict between the Cloud Act and European Law, in order to create sufficient safeguards and legal remedies against US surveillance measures and to ensure the protection of legal professional privilege and professional secrecy, the CCBE recommends that the EU takes the following steps:

1. Negotiate a mutual legal assistance treaty with the United States that explicitly refers to the Cloud Act, provides precise requirements for the transfer of data and does not undermine the level of protection provided by the fundamental freedoms;
2. Ensure that, according to such mutual legal assistance treaty, in each case, following a data request under the Cloud Act, data will be transferred only to the United States after there has been a notification to a competent and independent European authority;
3. Ensure that the affected service provider who is hosting the requested data is informed by the competent European authority about existing legal remedies in the United States;
4. Ensure that, according to such mutual legal assistance treaty, legal professional privilege and professional secrecy constitutes an absolute ground of objection to the transfer of data to the United States under the Cloud Act.

[33] https://uk.practicallaw.thomsonreuters.com/2-103-2508?transitionType=Default&contextData=(sc.Default&firstPage=true&bhcp=1