EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options
Theodore Christakis* and Fabien Terpan**

Key Points
- The EU and the US kicked off negotiations in September 2019 for the conclusion of a very important agreement on Law Enforcement Agents’ (LEA) access to data. This is the first article to present the context of these negotiations and the numerous challenges surrounding them.
- There are strong divergences between the EU and the US about what the scope and the architecture of this agreement should be. The US government supports the conclusion of a ‘framework agreement’ with the EU to be followed by bilateral agreements with EU Member States—in order to satisfy CLOUD Act requirements. The EU wishes to arrive at a self-standing, EU-wide comprehensive agreement and is opposed to solutions that might lead to fragmentation and unequal treatment between EU Member States.
- This article presents a detailed EU Law perspective on all these issues, and refers to relevant precedents concerning the conclusion of law enforcement, data-related or other international agreements. It discusses the division of competence on e-evidence between the EU and its Members States; possible architecture for the agreement and options under EU Law; and the role of the respective European Institutions (Commission, Council, Parliament) in the negotiation and conclusion of such an agreement.
- The article also studies, using existing case law, what the role of the Court of Justice of the European Union (CJEU) could be in relation to such an EU–US e-evidence Agreement.
- A post-scriptum also examines what the effects could be of the 16 July 2020 Schrems II Judgment of the CJEU on the ongoing EU–US negotiations, as well as the relevance of the 6 October 2020 data retention/collection judgments of the CJEU.
- The article will be useful to anyone interested in transatlantic data flows as well as judicial cooperation matters and, beyond its specific scope, could be used as a real ‘guide’ to EU Law procedures, options and precedents in relation to the conclusion of international data-related agreements.

Introduction
On 25 September 2019 the European Union (EU) and the USA officially started negotiations aimed at concluding a very important transatlantic agreement on cross-border access to electronic evidence (e-evidence) for judicial cooperation in criminal matters.1 Three...
There are a lot of extremely important and challenging issues of substance for the EU–US negotiations. The Covid-19 crisis has put the formal negotiation on hold but there is an expectation that they will resume soon.

Surprisingly, despite the importance of these negotiations, few if any academic articles have been written about them. The only exceptions, to our knowledge, are two pieces published well before the negotiations kicked off.

The first one is a brief paper by Jennifer Daskal and Peter Swire published in Lawfare in May 2018. This piece argues that the EU–US Agreement ‘is a good idea’, explains how the second part of the CLOUD Act operates in relation to the conclusion of executive agreements on e-evidence and advances the idea of a ‘framework agreement’ as a possible solution and architecture for the EU–US negotiations.

The second contribution was published by Peter Swire in the Cross Border Data Forum in April 2019. In this brief piece Swire ‘seeks to explain, especially for a non-U.S. audience, what it would mean under U.S. law to operate inside or outside of “the framework of the CLOUD Act”’. He presents the different options available for the architecture of the EU–US Agreement from the point of view of US law. Swire highlights that the intent of his article ‘is not to propose what legal instrument is desirable’ but rather to clearly expose what can be done within or outside of a CLOUD Act executive agreement.

The intention of the present study is to present an EU law perspective on all these issues so as to better understand the institutional constraints and possibilities of an EU–US agreement on Law Enforcement Agents’ (LEA) access to data. EU law (including EU external relations law) is particularly complex and it is necessary, both for a US and a European/international audience, to unravel these complexities and to present the EU mechanisms, procedures and requirements for an EU–US Agreement of access to e-evidence. Our intention is not to propose what legal instrument is desirable but, instead, to expose clearly, and from the point of view of EU law, what are the available options and architectures, and what could possibly challenge an EU–US agreement on e-evidence.

The discussion initiated by Daskal and Swire and continued here is important in our opinion. As we will see there are strong divergences on the desired architecture of the agreement between the EU and the US. The four negotiating sessions have until now concentrated on areas of substance (that will not be discussed as such in the present article) rather than the legal form of the agreement—and the intention on both sides is to continue discussing substantive issues rather than form and architecture when the negotiations resume. While this negotiating strategy is indisputably wise, issues of substance are closely related to issues of form and architecture. Indeed, the content of this data agreement could greatly vary depending on whether it is structured as a ‘framework’ agreement to be followed by bilaterals or as a comprehensive and self-standing agreement. Reports on divergences regarding these formal aspects pop up occasionally in the press. We thus consider that it is essential to explore the possible options for an EU–US agreement, which, in turn requires clarity on the procedures, requirements, and possibilities under both US and EU law.

To do so, we need to go back to the specific powers of the European Union as an external actor. Indeed, the EU is now a well-established actor in international relations, but it has not established this status without difficulty. Legal issues arise from the particularities of the EU as a legal entity. Three main features distinguish the EU from a state in the field of external relations. Contrary to a federal state where the federal government enjoys most of the external competence, in the European Union external competences are shared between the Union and the Member States. Another difference is to be found in the way the EU negotiates and concludes international agreements, and the variable role of the nature that the Member States play in this order to comply with European Human Rights Law (for instance: ensuring that data may not be requested for use in criminal proceedings that could lead to the death penalty); the willingness of the EU to introduce clauses in order to complement the Umbrella Agreement (see below the subsection ‘Existing EU–US law enforcement agreements’ (8)) with additional data protection safeguards; the determination of the EU to conclude an agreement that will be entirely reciprocal in terms of the rights and obligations of the parties and the categories of people whose data must not be sought pursuant to the agreement; and other issues. In this article we will not discuss these substantive issues, which deserve a separate article and analysis. We will only focus on problems of form, architecture, and procedure.

2 Jennifer Daskal and Peter Swire, ‘A Possible EU-US Agreement on Law Enforcement Access to Data’ (Lawfare, 21 May 2018) <https://www.lawfareblog.com/a-possible-eu-us-agreement-law-enforcement-access-data/> accessed 10 October 2020.

3 Clarifying Lawful Overseas Use of Data Act, [hereinafter CLOUD Act], contained in Consolidated Appropriations Act, 2018, PL 115-141, div. V. <http://www.crossborderdataforum.org/wp-content/uploads/2018/07/Cloud-Act-final-text.pdf/> accessed 10 October 2020.

4 Peter Swire, ‘EU and U.S. Negotiations on Cross-Border Data, Within and Outside of the CLOUD Act Framework’ (Cross Border Data Forum, 13 April 2019) <https://www.crossborderdataforum.org/eu-and-u-s-negotiations-on-cross-border-data-within-and-outside-of-the-cloud-act-framework/> accessed 10 October 2020.

5 There are a lot of extremely important and challenging issues of substance in the EU–US negotiations. These include: the procedural and fundamental rights safeguards that should be introduced in the agreement in order to comply with European Human Rights Law (for instance: ensuring that data may not be requested for use in criminal proceedings that could lead to the death penalty); the willingness of the EU to introduce clauses in order to complement the Umbrella Agreement (see below the subsection ‘Existing EU–US law enforcement agreements’ (8)) with additional data protection safeguards; the determination of the EU to conclude an agreement that will be entirely reciprocal in terms of the rights and obligations of the parties and the categories of people whose data must not be sought pursuant to the agreement; and other issues. In this article we will not discuss these substantive issues, which deserve a separate article and analysis. We will only focus on problems of form, architecture, and procedure.

6 See for instance ‘US Department of Justice has reservations about transatlantic agreement on access to electronic evidence’, Agence Europe, 21 November 2019.
process. Finally, the EU judicial system is also quite specific, with the Court of justice of the European Union acting like a quasi-constitutional court, trying to strike a balance between compliance with international law and the autonomy of the European legal order. These three characteristics will be used as a framework for the analysis of the EU–US negotiations on LEAs access to data.

The section ‘Setting the Scene’ of this article ‘sets the scene’ for the current EU–US data access negotiations by mapping previous EU–US law enforcement agreements, explaining why the conclusion of a new transatlantic agreement is considered necessary and exposing the divergence of views of the two sides on the architecture of the agreement.

The section ‘Issues of Competence’ focuses on issues of competence in EU law and explains the division of competence on e-evidence between the EU and its Member States and the consequences for transatlantic negotiations.

The section ‘Potential Agreement Structures’ presents the possible architecture of an EU–US LEAs access to data agreement under EU law based on previous analysis of competence sharing.

The section ‘Adoption of International Agreements by the EU: A Multi-Stage/Multi-Actor Process’ explains the procedure, under EU law, for the negotiation and conclusion of such a transatlantic agreement. It especially focuses on the role of the respective European institutions (Commission, Council, Parliament), how this could affect the progress of the negotiations and the voting majorities required for the conclusion of the agreement.

The section ‘The Eventual Role of the CJEU’ examines what eventual role the Court of Justice of the European Union (CJEU) could have in controlling such an EU–US data Agreement. Indeed, it has been said several times that the EU–US Agreement risks being deferred to the CJEU for judicial review. How could this happen (or not happen)? What are the different precedents and scenarios?

The article ends with a few thoughts on the future of the EU–US negotiations, including a post scriptum discussing briefly the potential effects of the Schrems II Judgment (Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems, Case C-311/18, ‘Schrems II’), issued by the CJEU on 16 July 2020, after the submission of this article.

Setting the scene

There are, as of today, at least eight important agreements on law enforcement that have been concluded between the EU and the US, which shows that transatlantic cooperation on these issues has been particularly fertile over the past 20 years (1). Despite this important existing network, new requirements have appeared with the passage of time and the negotiation of an agreement on cross-border access to electronic evidence has been deemed particularly important (2) despite initial divergences on what the precise objective and architecture of such an agreement could be (3).

Existing EU–US law enforcement agreements

In the period since the 9/11 2001 terrorist attacks the EU and the US have negotiated several agreements relevant for law enforcement. Here are eight of those agreements:

1. The Agreement between the USA and Europol,9 which was concluded in 2001, aimed ‘to enhance the cooperation of the Member States of the EU, acting through Europol, and the US in preventing, detecting, suppressing, and investigating serious forms of international crime’, in particular ‘through the exchange of strategic and technical information’.

2. The Supplemental Agreement between Europol and the USA on the Exchange of Personal Data and Related Information was concluded the following year, introducing a number of data protection safeguards not previously conceded by the US.

3. The Agreement on extradition between the EU and the USA (hereafter: EU–US Extradition). This Agreement, which was signed on 25 June 2003 and entered into force on February 2010, aims to enhance cooperation in terms of applicable extradition relations between EU Member States and the US constituted by an adequacy decision adopted by the Commission on 12 July 2016 (declaring that the US ensures an adequate level of protection as required by the Directive 95/46/EC) and a declaration and several letters issued by US authorities, and reproduced in the annexes. Whereas the adequacy decision was binding in the European Union, the documents issued by the US authorities were political engagements. cf Fabien Terpan, ‘EU-US Data Transfer from Safe Harbour to Privacy Shield: Back to the Square One’, (2018) 3(3) European Papers 1045–59. The Privacy Shield arrangement has been invalidated by the CJEU in its Schrems II Judgment of 16 July 2020 (see Post-Scriptum).

9 Agreement between the USA and The European Police Office signed on 6 December 2001.

We refer here to binding international agreements under International Law and art 2(1)(a) of the Vienna Convention on the Law of Treaties between States and International Organizations or between International Organizations, Vienna, 21 March 1968, UN Doc A/CONF. 129/15, 25 ILM 543 (1986).

One famous transatlantic instrument on cross border data issues was the EU–US Privacy Shield. However, it must be emphasized that Privacy Shield was neither related to law enforcement nor an international agreement (as defined in n 7). It was not a law enforcement instrument but instead was intended to offer protections in relation to government access to personal data transferred by companies to the USA for commercial purposes. And it was not an international agreement but just a transatlantic arrangement based on the passage of time and the negotiation of an agreement on cross-border access to electronic evidence has been deemed particularly important (2) despite initial divergences on what the precise objective and architecture of such an agreement could be (3).
governing extradition of offenders and replaces lists of offences that are deemed extraditable with a dual criminality standard.

4. The Agreement on mutual legal assistance between the EU and the USA (hereafter: EU–US MLA), signed and entered into force the same day as the EU–US Extradition. The MLA sets out conditions regarding the provision of mutual legal assistance in criminal matters between the EU and the US and seeks to enhance cooperation between EU countries and the US, complementing bilateral treaties between EU countries and the US.

5. The Agreement between the USA and Eurojust signed on 6 November 2006, the objective of which is to enhance cooperation between Eurojust and the US in combating serious forms of transnational crime including terrorism.

6. The Agreement between the EU and the USA on the processing and Transfer of Financial Messaging data from the EU to the US for the purposes of the Terrorist Finance Tracking Program (hereafter TFTP). This agreement, signed on 20 November 2009, organizes the transfer of international bank transfer data conducted through the SWIFT system, to US counter-terrorism authorities, while trying to preserve EU citizens’ privacy, especially by assessing whether the data requested in any given case is necessary for the fight against terrorism and the financing of terrorism.

7. The Agreement between the USA and the EU on the use and transfer of Passenger Name Record Data to the US Department of Homeland Security (hereafter: EU–US PNR). This agreement was signed on 14 December 2011 for the purpose of providing Passenger name records (PNR) from air carriers operating passenger flights to the US Department of Homeland Security in order to ‘ensure security and to protect the life and safety of the public’.

8. The Agreement between the USA and the EU on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, much better known as the ‘Umbrella Agreement’, signed on 2 June 2016. This Agreement aims to ensure that personal data is protected to a high standard when being transferred by law enforcement authorities (police and criminal justice authorities). It also aims to foster law enforcement cooperation between the EU and the EU countries, on the one hand, and the US on the other.

The number and importance of law enforcement agreements in force between the EU and the US, has prompted some scholars to observe that ‘this is arguably one of the most active fields of EU-US cooperation’. While transatlantic cooperation on law enforcement issues has been relatively successful, the conclusion of some of these agreements has been time-consuming or has proved controversial, attracting criticism by scholars, NGOs and even the European Data Protection Supervisor (EDPS). Despite this the EU and the US have always considered it necessary to continue to negotiate new ways forward that improve the scope and quality of transatlantic cooperation where law enforcement issues are concerned. For instance, in 2011 the EU and the US started negotiations aimed at putting in place a comprehensive high-level data protection framework for EU–US law enforcement cooperation. The result was the 2016 ‘Umbrella Agreement’ which intends to provide safeguards and guarantees of lawfulness for data transfers and to guarantee that all EU citizens have the right to enforce data protection rights in US courts, whether or not they reside on US soil.

---

10 Elaine Fahey, ‘The Evolution of Transatlantic Legal Integration: Truly, Madly, Deeply? EU – US Justice and Home Affairs’ in A Ripoll Servent and F Trautner (eds), The Routledge Handbook of Justice and Home Affairs Research (Routledge, London 2017), at 587. See also: Elaine Fahey and Deirdre Curtin (eds), A Transatlantic Community of Law: Legal Perspectives on the Relationship between the EU and US Legal Orders (CUP, Cambridge 2014); Elaine Fahey, ‘Transatlantic Cooperation in Criminal Law’ in M Bergström, V Mitsilegas and T Konstadinides (eds), Research Handbook on EU Criminal law (Edward Elgar, Cheltenham 2015), at 11 (stating that: ‘An examination of contemporary practice reveals much “sophistication” in the evolution of transatlantic criminal law cooperation. It appears perhaps even disproportionately extensive, relative to the many limitations of mutual recognition in justice’).

11 Fahey, ibid, at 537 has observed in relation to the 2003 extradition and MLA Agreements that ‘the secrecy of the negotiation of the agreements and their limited review by parliaments in both jurisdictions gave rise to concerns about the democratic character of the agreements. Similarly, the omission of human rights protections from the scope of the agreements provoked concerns, as did the prospect of joint investigation teams working together as well as the place of personal data within the scope of the agreements’. The PNR and TFTP agreements have also generated controversy especially on account of their limitations on redress and their uneven application of US law to EU citizens, not enabling the latter to fully realise their rights to redress and review. Even the more recent Umbrella Agreement, which intends inter alia to deal with these issues, has been criticized by NGOs (see for instance Fanny Hidvegi and Estelle Massé, ‘The Umbrella Agreement Just Isn’t Good Enough to Protect our Rights’ (24 November 2016) <https://www.accessnow.org/umbrella-agreement-just-Isn’t-good-enough-protect-rights/> accessed 10 October 2020).

12 For criticism of the Umbrella Agreement by the EDPS see Opinion 1/2016, Preliminary Opinion on the agreement between the US and the EU on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences, 12 February 2016.
More recently, a transatlantic agreement on cross border access to e-evidence has also been considered a pressing need.

The Need for an EU–US agreement on cross border access to electronic evidence

It has been noted that ‘increasingly, evidence critical to ordinary criminal investigations is located across territorial borders. Before the rise of cloud computing, evidence of crimes generally was available within the requesting country’s territorial jurisdiction. Today, the content of emails, social network posts, and other content are often stored in a different country’. A 2018 report by the European Commission found that electronic evidence is needed in around 85 per cent of all criminal investigations, and in two-thirds of these investigations there is a need to obtain evidence from online service providers based in another jurisdiction.

This globalization of criminal evidence is creating significant challenges for law enforcement. Traditional cross-border mechanisms such as Mutual Legal Assistance Treaties are widely considered too slow and cumbersome. Countries around the world are responding with new laws and legal instruments to deal with the situation.

In the US, Congress adopted the CLOUD Act in March 2018. The first part of this Act mooted the pending Supreme Court case of United States v Microsoft, stating that the kind of compelled disclosure orders at issue in the Microsoft Ireland case apply ‘regardless of whether such communication, record, or other information is located within or outside of the United States’. The second part of the CLOUD Act creates a new mechanism for other countries to access the content of communications held by US service providers. It enables the US to reach ‘executive agreements’ with certain ‘qualified’ foreign governments, permitting, subject to a number of baseline substantive and procedural requirements, the lifting of blocking provisions imposed due to the Electronic Communications Privacy Act (ECPA) and enabling the law enforcement agencies of these countries to request communications content of non-US citizens and residents directly from service providers.

Just a few weeks later, on 17 April 2018, the EU commission introduced ‘E-Evidence’, its own legislative package which aims to streamline cooperation within the EU with service providers and supply law enforcement and judicial authorities with expeditious tools to obtain e-evidence. The Council adopted its E-Evidence draft in December 2018 while the Rapporteur of the LIBE Committee Birgit Sippel presented her draft report on E-Evidence on November 2019. Delayed due to the Covid-19 crisis and lockdowns, discussions in the European Parliament are expected to resume soon and we might have the trilogues during the first half of 2021.

It is against this context that the EU and the US felt the need to start discussing a transatlantic agreement without waiting for the adoption of E-evidence. Indeed, while the Commission and the Council emphasized several times that the EU–US Agreement could only be

13 Peter Swire, Theodore Christakis and Jennifer Daskal, ‘The Globalisation of Criminal Evidence’ (IAPP Privacy Tracker, 16 October 2018) <https://iapp.org/news/a/the-globalization-of-criminal-evidence/> accessed 10 October 2020.

14 See European Commission Staff Working Document, Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings [2018] <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN> accessed 10 October 2020.

15 Theodore Christakis, ‘Data, Extraterritoriality and International Solutions to Transatlantic Problems of Access to Digital Evidence. Legal Opinion on the Microsoft Ireland Case (Supreme Court of the United States)’ (29 November 2017), The White Book. Lawful Access to Data: The US v. Microsoft Case, Sovereignty in the Cyber-Space and European Data Protection, CEIS & The Chertoff Group White Paper (December 2017). <https://ssrn.com/abstract=3086820> accessed 10 October 2020.

16 A first such ‘CLOUD Act executive agreement’ was concluded between the US and the UK in October 2019 and entered into force on 8 July 2020 (Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, 3 October 2019). For an analysis of the UK–US Agreement see, eg Jennifer Daskal and Peter Swire, ‘The UK-US CLOUD Act Agreement is Finally Here, Creating New Safeguards’ Lawfare and Just Security blog, 8 October 2019. <https://www.justsecurity.org/66507/the-uk-us-cloud-act-agreement-is-finally-here-containing-new-safeguards/> accessed 10 October 2020; Theodore Christakis, ‘21 Thoughts and Questions about the UK-US CLOUD Act Agreement’ European Law Blog, 17 October 2019 <https://europeanlawblog.eu/2019/10/17/21-thoughts-and-questions-about-the-us-cloud-act-agreement-and-an-explanation-of-how-it-works-with-charts/> accessed 10 October 2020; Theodore Christakis and Kenneth Propp, ‘The Legal Nature of the UK-US CLOUD Agreement’ (Cross Border Data Forum, 20 April 2020) <https://www.crossborderdataforum.org/the-legal-nature-of-the-uk-us-cloud-agreement/> accessed 10 October 2020. The US is about to negotiate another CLOUD Act executive agreement with Australia.

17 See European Commission, ‘E-Evidence’ <https://ec.europa.eu/home-affairs/what-we-do/policies/organised-crime-and-human-trafficking/e-evidence_en/> accessed 10 October 2020.

18 See Theodore Christakis, ‘E-Evidence in a Nutshell: Developments in 2018, Relations with the CLOUD Act and the Bumpy Road Ahead’ (Cross Border Data Forum, 14 January 2019) <https://www.crossborderdataforum.org/e-evidence-in-a-nutshell-developments-in-2018-relations-with-the-cloud-act-and-the-bumpy-road-ahead/> accessed 10 October 2020.

19 See Theodore Christakis, ‘Lost in Notification! Protective Logic as Compared to Efficiency in the European Parliament’s E-Evidence Draft Report’ (Cross Border Data Forum, 7 January 2020) <https://www.crossborderdataforum.org/lost-in-notification-protective-logic-as-compared-to-efficiency-in-the-european-parliaments-e-evidence-draft-report/> accessed 10 October 2020.
could permit this problem to be addressed and minimize or even eliminate conflicts of laws by allowing US service providers to deliver content data directly to EU LEAs.

On the other hand, the first part of the CLOUD Act, authorizing US LEAs to request data relevant to criminal investigations from CSPs ‘regardless of whether such communication, record, or other information is located within or outside of the United States’, might conflict with existing European law (including the GDPR25 or national blocking statutes) in some situations and especially when the requests concern personal data of Europeans. This issue has been analysed by legal scholars26 while the European Data Protection Board (EDPB) and the EDPS have also published a joint position on this.27

The conclusion of an EU–US Agreement thus appears the only way to resolve the problem of conflicts of laws in the interest of the EU and its Members States, the US and US and European CSPs. As noted by the Commission,28 such an agreement would also offer a number of other practical advantages including improving timely access to data for judicial authorities and clarifying the binding nature and enforcement of orders on service providers while also specifying judicial authorities obligations.

EU/US divergence of views on the architecture of the agreement

While both sides agree on the importance of an EU–US Agreement, there are strong divergences about the scope29 and architecture of such an Agreement.

20 A point reiterated once again on 4 June 2020 by the European Commissioner for Justice, Didier Reynders. See “Real” negotiations with United States over E-evidence will only take place when agreement is reached on European side according to Didier Reynders’, Europe Daily Bulletin No12499, Agence Europe.
21 Council of European Union’s Decision of 6 June 2019 authorizing the opening of negotiations in view of an agreement between the EU and the USA on cross-border access to electronic evidence for judicial cooperation in criminal matters, <https://data.consilium.europa.eu/doc/document/ST-9114-2019-INIT/en/pdf> accessed 10 October 2020.
22 Addendum to the 6 June 2019 Council Decision, <https://data.consilium.europa.eu/doc/document/ST-9666-2019-INIT/en/pdf> accessed 10 October 2020. These directives set a series of conditions on the nature and scope of the Agreement that the Commission should follow as well as a series of procedural and other fundamental rights safeguards that should be introduced in the agreement to comply with EU law (see n 5).
23 Recommendation for a Council decision authorizing the opening of negotiations in view of an agreement between the EU and the USA on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM/2019/70 final, Brussels, 5 February 2019. See also European Commission, ‘Questions and Answers: Mandate for the EU-U.S. Cooperation on Electronic Evidence’ (5 February 2019) <https://ec.europa.eu/commission/presscorner/detail/en/MEMO_19_863> accessed 10 October 2020.
24 Other reasons include the necessity of putting some order in the practice of ‘voluntary cooperation’ with service providers for LEAs access to non-content data. The Commission notes that the scale of direct cooperation requests on a voluntary basis has rapidly increased with more than 124 000 in 2017. However, direct cooperation on a voluntary basis for non-content data ‘can be unreliable, it may not ensure respect of the appropriate procedural safeguards, is only possible with a limited number of service providers which all apply different policies, is not transparent and lacks accountability’. The resulting fragmentation ‘may generate legal uncertainty, raise questions on the legality of prosecution as well as concerns on the protection of fundamental rights and procedural safeguards for the persons related to such requests’. See Recommendation for a Council decision . . . (ibid). An EU–US Agreement could permit these issues to be addressed.
25 European Parliament and Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.
26 Theodore Christakis, ‘Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: Is There a Conflict with the GDPR?’ in Randal Milch, Sebastian Benthall and Alexander Poitcovaru (eds), Cybersecurity and Privacy in a Globalized World - Building Common Approaches (New York University School of Law, e-book, 2019) 60–76. <https://ssrn.com/abstract=3397047> accessed 10 October 2020.
27 EDPB–EDPS, ‘Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection’ (10 July 2019) <https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb–edps-joint-response-libe-committee-impact-us-cloud-act_fr> accessed 10 October 2020.
28 Recommendation for a Council decision . . . (n 23).
29 Beyond the elements discussed in this section, a very important challenge related to the scope of the EU–US Agreement concerns the relationship between the two parts of the CLOUD Act and whether the US would still be able to use the first part of the CLOUD Act after the conclusion of an
For the US, the architecture should take into account some important CLOUD Act requirements and restrictions.

First, the CLOUD Act authorizes the conclusion of an executive agreement with ‘a foreign government’ only. It is far from clear whether the US could conclude a CLOUD Act Agreement with the EU itself—and under which conditions.

Secondly, and most importantly, the CLOUD Act requires each ‘foreign government’ to be certified by the Attorney General, with the concurrence of the Secretary of State, as affording ‘robust substantive and procedural protections’ with respect to privacy and civil liberties in its ‘domestic law’, among multiple other requirements. As explained by Daskal and Swire, ‘this suggests, at a minimum, that the US must undertake and produce an inquiry, analysis, and finding with respect to the domestic legal system of each member-state or subunit thereof with which the United States would enter into an agreement. We do not see a convincing read of the statute that can bypass this requirement’.

As a solution to this problem Daskal and Swire envision two possible options. Either the EU and the US negotiate an agreement outside the CLOUD Act—but this would require taking into consideration the constraints and approval process of treaties imposed by US constitutional law; or the EU and the US opt for a CLOUD Act executive agreement (which could greatly facilitate and accelerate the process of its entry into force) but in such a case the only solution would be to conclude a ‘framework agreement’ which would set out a series of rules and procedures applicable to the relations between the US and EU Member States but which would not be self-standing without additional agreement relations with specific Member States. Daskal and Swire do not clearly indicate whether they envision an EU–US ‘framework agreement’ followed by bilaterals (as occurred with the MLA or extradition agreements), or, instead, a single complex instrument which would include both the EU and Member States ‘qualified’ by the US. However, they seem to have a preference for the latter when they write that “This framework approach has the advantage of allowing the U.S. to negotiate one general agreement, pursuant to which each EU member-state could individually accede31 and this idea seems to be reinforced when Swire refers to a ‘negotiation at the EU level but additional steps needed for ratification by each Member State’.32 What seems essential to them is to find an architecture that would allow the US to provide a ‘separate certification for each member-state’.

The ‘framework agreement’ idea has been adopted by the US delegation. At the opening of negotiations in September 2019, the US clearly ‘stressed that their objective was to negotiate a framework agreement supplemented by bilateral agreements with individual EU Member States’.33

More recently, Richard Downing, Deputy Assistant Attorney General, expressed his reservations about the feasibility of an EU–US Agreement precisely because of the CLOUD Act requirements. He stressed that the US justice system is obliged to ensure beforehand that each foreign partner complies with the standards and rules required by the CLOUD Act. ‘These are difficult standards to meet’, said Richard Downing. ‘There are some countries in the world that we do not expect any time soon to be able to sign one of those agreements, because they do not have the same respect for the rule of law, and privacy and civil liberties’ he said, eventually referring to rule of law problems in a few European countries being an issue of concern for the US.34 And he concluded by saying that ‘he is not certain that a single agreement, valid for all European countries, can be reached’, but ‘there is a possibility that we might have a sort of framework agreement where we resolve many issues at the EU level, and then have individual agreements with Member States to resolve the remaining issues’. He referred to the EU–US MLA and the bilateral Mutual Legal Assistance Treaties (MLATs) as a precedent.35

Against this background, the EU wishes to conclude a self-standing, EU-wide comprehensive agreement. During the opening of the negotiations the EU stressed this point and emphasized that ‘it had a mandate to conclude an EU-wide agreement’.36 The Commission

31 Daskal and Swire (n 2).
32 Swire (n 4).
33 Report from the Commission on the opening of negotiations in view of an agreement between the EU and the US on cross-border access to electronic evidence for judicial cooperation in criminal matters, 12524/19, 25 September 2019, at 3.
34 See below the subsection ‘A comprehensive self-standing EU agreement’.
35 ‘US Department of Justice has reservations about transatlantic agreement on access to electronic evidence’, Agence Europe, Europe Daily Bulletin No 12374 (21 November 2019).
36 Report from the Commission... (n 33), at 2.
emphasized several times that ‘to avoid fragmentation and different levels of protection in different EU Member States there should be a common EU approach rather than bilateral agreements between the US, third countries and some EU Member States’.

As a matter of policy and as the negotiation mandate indicates, the EU considers it difficult to engage in a process with a third country leading to a legal regime that would treat EU countries unequally. The EU is concerned that this would lead to fragmentation and might eventually replicate a situation similar to the Visa Waiver Program (VWP) that has led to a lot of criticism within the EU. Indeed, visa reciprocity is a fundamental principle of the EU’s common visa policy and an objective that the Union pursues in a proactive manner in its relations with non-EU countries. This principle means that the EU, when deciding whether to lift visa requirements for citizens of a non-EU country, takes into consideration whether that non-EU country reciprocally grants visa waivers to nationals of all EU Member States. In April 2014 the European Commission was made aware that the US—along with Australia, Brunei, Canada, and Japan—was failing to ensure the same visa waiver rights for its citizens that Europe offered in return. The Commission then gave these countries a deadline of two years before it said it would retaliate. Since then, Australia, Brunei, Canada, and Japan have all lifted their visa requirements, but the US has failed to act. The State Department’s Bureau of Consular Affairs has said in the past that Bulgaria, Croatia, Cyprus, Poland, and Romania do not yet meet security requirements for the US VWP. In response, a 2017 European Parliament resolution asked for the reintroduction of visas for citizens from the USA. This idea was abandoned, but the problem remains and the EU certainly does not want to replicate this situation and be dependent on unilateral US ‘certifications’ in terms of e-evidence. This is probably the reason why the European Parliament recommended negotiating an agreement outside the framework of the CLOUD Act.

Having thus presented the policy desires of each side, let’s now turn to EU law to see what the available options are and how exactly these desires could be implemented in practice.

### Issues of competence

As rightly noted by Swire and Daskal ‘EU Law contains its own complexities about whether and to what extent the EU can be a counter-party for negotiations of executive agreements under the CLOUD Act’. Indeed the EU, although enjoying international legal personality, is composed of Member States who continue to make international commitments in many areas. It is thus necessary to start with a number of observations on the respective role of the EU and its Member States. While the EU and Member States enjoy a shared competence in the Area of Freedom, Security and Justice (AFSJ) (1), the margin of intervention of individual Member States (for example to negotiate simultaneously bilateral agreements with the US) is limited once the EU has exercised its competence at European level (2).
A shared competence...

The EU’s legal capacity to conclude an international agreement with regards to e-evidence issues may directly derive from the EU Treaties: areas such as development cooperation, commercial policy, humanitarian assistance, and the Common Foreign and Security Policy have specific legal bases in EU primary law. But in many cases the external capacity of the EU mirrors its internal capacity, as the European Court of Justice stated in its early case law.46

E-evidence is part of the Area of Freedom, Security and Justice, a competence shared by the EU and its Member States. The proposal for a regulation on e-evidence, issued by the Commission in April 2018, is based on Article 82 of the Treaty on the Functioning of the European Union (TFEU)47 (judicial cooperation), according to which measures may be adopted in accordance with the ordinary legislative procedure to lay down rules and procedures to ensure recognition throughout the Union of all forms of judgments and judicial decisions. As this proposal concerns cross-border procedures, where uniform rules are required, there is no need to leave a margin for Member States to transpose such rules, hence the choice of a regulation instead of a directive.48 Thus, the EU has started to use its specific competence in the field of e-evidence, and this in turn has a direct impact on the way the EU and Member States can intervene externally in this very same field.

But when the EU starts working on an issue, the MS capacity to act is limited

Criminal matters are not an exclusive competence of the European Union, so in theory bilateral agreements between the US and EU Member States, and even mixed agreements, are possible. However, under EU law, the Member States’ external competence would appear to be limited for a series of reasons.

First, the European Union is endowed to sign an EU-wide agreement on e-evidence with the US, negotiated by the Commission, with no direct individual participation of the Member States required. Just as with the EU-US MLA agreement,49 agreement on e-evidence will be concluded by the EU in the same way, and should not be considered as a mixed agreement50 defined as treaties to which the EU and at least some of its Member States are parties.

The approach of the Commission on e-evidence is to address any conflicts of law within and outside the EU. For the EU it is necessary to adopt common rules regarding cross-border access to electronic evidence and to have a common approach and legal regime both within the EU and in relation to third countries, starting with the US (who is a particularly important partner, taking into consideration the fact that most CSPs are American). This willingness to adopt common rules is all the more pressing when one takes into account the fact that EU-US negotiations concern not only cooperation in criminal matters but also, simultaneously, data protection issues.51

Hence, by legislating on e-evidence, the EU has bolstered its capacity to commit at the international level. As Article 3(2) TFEU says, ‘The Union shall also have exclusive competence for the conclusion of an international agreement when its conclusion is provided for in a legislative act of the Union or is necessary to enable the Union to exercise its internal competence, or in so far as its conclusion may affect common rules or alter their scope.’ Since e-evidence is intended to be covered by an EU regulation, it means that the European Union will have used its competence in this field, reducing the MS marge of manoeuvre to a point that the EU–US agreement on e-evidence falls into the category of exclusive competence of the EU.52

Another consequence of EU legislation is that negotiating individual bilateral agreements with the US would...
be problematic and could only occur in conformity with European Law. At this stage, we must distinguish between two main periods: before and after the entry into force of the regulation and the conclusion of an EU–US agreement.

If a Member State starts negotiating a bilateral agreement with the US before the regulation on e-evidence is in force and the EU–US negotiations are concluded, this could be seen as a breach of the principle of sincere cooperation (Article 4(3) of the Treaty of the European Union, TEU) which states that ‘The Member States shall facilitate the achievement of the Union’s tasks and refrain from any measure which could jeopardise the attainment of the Union’s objectives’). As Eeckhout summed it up: ‘unilateral treaty making action by a Member State coinciding with EU negotiation cannot be tolerated, unless that Member State consults and cooperates with the EU, and in particular with the Commission’. It is not only EU positive law but also ‘future developments’ of EU law that need to be taken into account during the negotiations of external agreements. This prevents the Member States from acting in a way that could jeopardize the negotiation process led by the Commission.

In July 2019 the EU Commissioner on Justice, Věra Jourová, urged US authorities to refrain from negotiating separate bilateral agreements with Member States. As a consequence, in the event of unilateral action the Commission could take measures, starting with a letter sent to the Member State concerned. The issue could also be discussed in a meeting of the Council of ministers or could even be raised at Head of state or government level.

If such a bilateral agreement was signed regardless, the Commission could assess whether Union law had been complied with, notably the GDPR and the European Charter of Fundamental Rights, and even decide to start an infringement procedure. The issue was raised when the UK, which was still a member of the EU at that time, signed an agreement with the US under the CLOUD Act. The possibility of the Commission taking appropriate measures was confirmed by Mr Reynders, the new Commissioner for Justice, in an answer given to a written question by MEPs Moritz Körner and Sophia In’t Veld.

Once the regulation is in force and the EU–US Agreement is concluded, it can be argued that Member States have lost the competence to negotiate individual agreements with the US. The share of competences between the EU and Member States is constantly evolving: the more the EU uses its competence, the less Member States are able to act on their own, be it via legislation or international agreements. An agreement between a Member State and the US could be challenged on the grounds of competence and challenged for being in violation of Union law, including the EU regulation on e-evidence.

After the conclusion of the EU–US agreement, concern about competence would thus be even stronger. A Member State–US agreement could only be concluded in compliance with Union law if it took into account both EU regulation and the EU–US agreement. In other words, Member States would still be able to negotiate an agreement with the US but under two conditions: (i) Either they negotiate on areas which are not covered by EU law; or (ii) They negotiate on areas covered by EU law but on condition that the EU–US Agreement authorizes this and does so within the limits fixed by this authorization—which is what happened, for example, in the fields of extradition and Mutual Legal Assistance as we will now see.

**Potential agreement structures**

In light of the above and the EU external relations legal framework, there are theoretically four basic options for an EU–US Agreement (although each of them could include internal variations).

---

53 In Case C-246/07, Commission v Sweden, the Court examined in detail the duty of sincere cooperation in relation to Member State action in international fora. See Marise Cremona, ‘Case C-246/07, Commission v. Sweden (PFOS), Judgment of the Court of Justice (Grand Chamber) of 20 April 2010’ (2011) 43 Common Market Law Review 1639–65.

54 Piet Eeckhout, *EU External Relations Law* (2nd edn, OUP, Oxford 2011), at 248.

55 To assess whether an area is largely covered by common rules, account must be taken not only of EU law as it currently stands, but also of its future development, in so far as that is foreseeable (Case C-66/13 Green Network, EU:C:2014:2399, paras 61–64; Opinion 1/03 (New Lugano Convention), EU:C:2004:490, para 126).

56 Hearing before the LIBE Committee, 25 July 2019, Agence Europe, no 12304.

57 See n 16.

58 See Question reference E-003136-19, date of the parliamentary question 7 October 2019, date of the written answer: 10 January 2020; <https://www.europarl.europa.eu/doceo/document/E-9-2019-003136_EN.html> accessed 10 October 2020.
Excluding the MoU scenario

Concluding a Memorandum of Understanding (MoU) is a scenario which can be excluded. A MoU is an instrument of soft law often used when parties cannot or are not willing to come to a legally enforceable agreement. They want to express their common intention to reach certain objectives without committing in a proper legal manner.

Concluding a MoU is usually faster than concluding a formal agreement and cannot be challenged before a court due to its non-binding nature. Although the use of soft law is growing in the European Union, the form that the MoU takes does not reflect the intentions of EU institutions in the field of external relations, the competence of the EU. And the negotiation of the EU–US agreement is conducted by the Commission alone.

The mixed agreement scenario

A second scenario is one involving a ‘mixed agreement’. As mentioned above, a mixed agreement is signed by both the EU and Member States in areas of shared competences. Not only the EU but Member States are contracting parties, and the Commission is not the only negotiator.

Theoretically AFSJ is a shared competence, so the conclusion of a ‘mixed agreement’ could have been envisaged in the case of e-evidence. Admittedly, the spectrum from exclusive to mixed agreement is rarely crystal-clear and often has an explicit political dimension. However, with the commencement of a legislative process on the matter, the decision has been made to conclude an EU-wide agreement falling within the exclusive competence of the EU. And the negotiation of the EU–US agreement is conducted by the Commission alone.

It is true that the legal status of an agreement can change during the negotiation. The Comprehensive Economic and Trade Agreement between the EU and Canada was considered by the Commission as falling under the exclusive competence of the EU, but several national parliaments and governments, together with the EU Council of Foreign Affairs, pushed in favour of its classification as a mixed agreement, which was finally accepted by the Commission when the latter proposed a different signature and conclusion of the agreement to the EU Council. But the situation was different as the CETA goes beyond the traditional scope of a trade agreement and includes an investment chapter that justifies the ‘mixed’ classification.

The content of the EU–US agreement on e-evidence is different. Obviously, it is not being negotiated as a mixed agreement and there is no intention whatsoever to re-classify it as a mixed agreement.

In any case, having recourse to the mixed procedure does not seem to be of any interest to the contracting parties.

The EU has never used the mixed agreement form in any of its law enforcement or data-related agreements with the US and other States, and is searching for legal consistency between its internal and external rules on the matter. Transforming the EU–US Agreement on LEA access to data into a ‘mixed agreement’ might only create unwelcome problems and complications. Member States will all need to sign and ratify such a mixed agreement following their sometimes complex and time-consuming internal procedures, which could be a source of unnecessary delays. Theoretically, one should not deny that there could be further complications if the Parliament in a specific country is sceptical about the new forms of law enforcement access to data envisioned by the agreement and their effects on data protection and human rights (although it could be argued that there is a duty to ratify when there is strong EU interest for the agreement to enter into force).

For the US, one main advantage of the mixed procedure would be that such an agreement, where both the EU and its Member States are parties, would clearly align with the CLOUD Act’s formal requirement that executive agreements can only be concluded with ‘foreign governments’. On the other hand, recourse to the mixed procedure would not in principle give any power to the US to proceed to a separate ‘certification’ (in respect of CLOUD Act requirements) for each EU

59 Fabien Terpan, ‘Soft Law in the European Union, The Changing Nature of EU Law’ (2015) 21(1) European Law Journal 68–96.
60 Ramses A Wessel, ‘Normative Transformations in EU External Relations: The Phenomenon of “soft” International Agreements’ (2020) West European Politics 1–21.
61 The ECPA requires a binding international agreement in order to lift the bar on disclosure to foreign governments. A soft law approach cannot repeal the ECPA requirements and would be pointless.
62 cf Marcus Klamer, The Principle of Loyalty in EU Law (OUP, Oxford 2014) at 203.
Member State. Normally, recourse to the mixed procedure will not give any power to the US to ‘pick and choose’ EU Member States; it would be either all or nothing.

A comprehensive self-standing EU agreement

In areas where the EU has an exclusive competence, or when there is a shared competence but the EU has bolstered its capacity to commit at the international level (as envisioned in Article 3(2) TFEU and discussed above in the subsection ‘But when the EU starts working on an issue, the MS capacity to act is limited’) the EU has the capacity to negotiate and conclude alone an EU-wide, self-standing agreement. In such a case Member States play no autonomous role in the negotiation or conclusion of such an agreement, and they do not become parties to it. When such an agreement enters into force between the EU and the third State, it becomes immediately binding on all Member States as a matter of EU law.

Several EU–US law enforcement agreements have followed this structure. This is the case for all EU–US agreements concluded since the entry into force in 2009 of the Lisbon Treaty: the 2009 TFTP Agreement; the 2011 PNR Agreement; and even the 2016 Umbrella Agreement.

As mentioned earlier (I(3)) the EU wishes that the transatlantic agreement on cross-border access to electronic evidence also follows this structure. However, as has also been mentioned, this creates difficulties for the US. There is a lot of uncertainty as to whether the CLOUD Act can authorize the conclusion of an agreement with the EU only. Beyond this legal issue, the US is concerned that the conclusion of an Agreement with the EU as a whole will not give power to the US to ‘pick and choose’ EU Member States, and would also present, eventually, other operational advantages for the US side.

An EU agreement followed by bilaterals

Another option is to conclude an EU–US Agreement followed by bilateral EU–US Agreements with EU Member States. This is the preferable option for the US as such a structure would most accurately meet the US CLOUD Act requirements of qualified ‘foreign govern-ments’ certification. This would in turn permit the US Government to avoid concluding bilateral agreements with EU Member States where there are rule of law problems and would also present, eventually, other operational advantages for the US side.

Two important precedents exist here in relation to the extradition/MLA Agreements. The EU–US negotiations on these issues started in the spring of 2002 and the two agreements were signed by the US and the EU in record time, on 25 June 2003. However, their entry...
into force only occurred seven years later after the conclusion of a dense network of bilateral agreements between the US and EU Member States. As a matter of fact, in addition to the two overarching agreements with the EU, the US and each of the EU Member States have either entered into new agreements or adopted changes to existing extradition and mutual legal assistance agreements to meet the new requirements. In total, 56 new treaties were negotiated, and the US Senate gave advice and consent to them in the autumn of 2008. After EU Member States completed their ratifications, EU and US authorities exchanged their instruments of ratification on 28 October 2009. The agreements entered into force in February 2010, 8 years after the negotiations kicked off.

The EU–US extradition and MLA agreements were thus clearly ‘framework agreements’, providing a common framework and content for MLA and extradition rules in relation to the individual agreements between individual Member States and the US. The EU–US agreements did not entirely replace existing bilateral Treaties but rather amended and supplemented them. Both agreements also clearly stated that they ‘shall not preclude the conclusion, after [their] entry into force, of bilateral agreements between a Member State and the US consistent with this Agreement’.67

In other words, the framework EU–US agreements set minimum and common rules that must be respected by the US and the Member States when negotiating their respective bilateral instruments. As two authors observed, this type of agreement ‘is a clear expression of the division of tasks between Member States and the EU in respect of many AFSJ fields: the EU as a norm-setting authority, with enforcement-related rules carried out by Member States’.68

However, this process is time-consuming as it requires the conclusion of an Agreement both with the EU and with Member States. In the MLA/extradition precedents it took 8 full years for the agreements to enter into force. And let’s not forget that with the EU–US LEA access to data agreement things could get even more complicated as: (i) The EU–US Agreement cannot be concluded before the adoption of e-evidence legislation at EU level (a complicated and time-consuming process in itself); and (ii) Bilateral agreements cannot be negotiated before the adoption of the EU–US Agreement. Waiting years for the creation of an effective transatlantic legal regime could be detrimental for all stakeholders: the EU, the US but also, most of all, service providers who might find themselves trapped in an increasing number of conflicts of laws. As discussed above, contrary to the EU–US MLA agreement, the signing of bilateral treaties between the US and individual Member States is not foreseen by the EU.

Furthermore, the extradition/MLA Agreements ‘model’ has come about due to very specific historical circumstances which are different to the LEA access to data case. In particular, at the time of the negotiation of the EU–US extradition and MLA Agreements, there were already several pre-existing bilateral agreements between the US and some EU Member States. Negotiations at the EU–US level had to take this reality into consideration.

Interestingly, the MLA Agreement with Japan69 contrasts with the EU–US MLA. The Agreement with Japan contains no clause on subsequent bilateral implementation agreements and must therefore be understood as a self-standing agreement70 which nonetheless contains the statement that ‘nothing in this agreement shall prevent a Member State and Japan from concluding international agreements confirming, supplementing, extending or amplifying the provisions thereof’.71

Adoption of international agreements by the EU: a multi-stage/multi-actor process

As we have seen in the previous section, all possible options imply the conclusion of an agreement (either of a ‘comprehensive/self-standing’ or ‘framework’ agreement) between the EU and the US. Therefore, it is important to examine now how an international agreement is concluded under EU law and the exact roles of the different European Institutions involved.

The procedural legal basis for working towards, signing and concluding most EU international agreements, including the EU–US agreement on e-evidence, is Article 218 TFEU, which lays down a complex multi-stage process involving the Commission, the Council and the Parliament.72

---

67 Bart Van Vooren and Ramses A Wessel, EU External Relations Law: Text, Cases and Materials (CUP, Cambridge 2014) 431. See also: Ramses A Wessel and Joris Larik (eds), EU External Relations: Text, Cases and Materials (Hart, Oxford/London/New York 2020).
68 Agreement between the EU and Japan on mutual legal assistance in criminal matters, signed on 15 December 2009 and entered into force just a year later (on 2 January 2011).
69 Van Vooren and Wessel (n 68) 431.
70 Art 27(2) of the Agreement.
71 Piet Eckhout, EU External Relations Law (2nd edn, OUP, Oxford 2011); Panos Koutrakos, EU International Relations Law (Hart Publishing, Oxford 2015); Joris Larik and Ramses A Wessel, ‘Instruments of EU External Action’ in Wessel and Larik (n 68), at 101; Marc Maresceau and Alan Dashwood, Law and Practice of EU External Relations: Salient Features of a Changing Landscape (CUP, Cambridge 2008).
Opening of negotiations

Article 218(2) TFEU requires the Council of ministers to authorize the opening of negotiations and adopt negotiating directives. This decision may be preceded by a high-level political request from EU Heads of state and government. In its conclusions adopted on 18 October 2018, the European Council stated that: ‘solutions should be found to ensure swift and efficient cross-border access to electronic evidence in order to effectively fight terrorism and other serious and organised crime, both within the EU and at international level’.

The Commission contributed to the definition of its own mandate by proposing to start international negotiations on 5 February 2019 and by submitting recommendations to the Council of ministers as set out in Article 218(3) TFEU. Vera Jourová, the then Commissioner in charge of justice, started informal talks with William Barr, the US Attorney General, during a visit from 10 to 12 April 2019.

On 6 June 2019, the Justice and Home Affairs Council finally adopted the Decision authorizing the opening of negotiations and agreed on the negotiating directives for the Commission as the EU’s negotiator.

While it has no formal role in the opening of negotiations vis-à-vis an international agreement put forward by the EU, the Parliament could have issued a resolution on this matter asking the Commission to include the Parliament’s concerns in its recommendation to the Council; it refrained from doing so. In September 2019, formal negotiations between the Commission and the US Department of Justice began.

Conduct of negotiations

Given that the Commission is in charge of conducting negotiations, it plays a key role in the process under the watchful eye of the Member States and the Parliament.

In practice, the Commission keeps the Council informed periodically. The negotiation directives of June 2019 also require that the Commission report to the Council on the outcome of each negotiating session. The progress of the negotiation is reviewed at ministerial level. The Commission’s room for manoeuvre can be extended in practice, via diplomatic skills, but there are strong limitations to this due to both the EU legislation in operation and the position of the Council. More specifically, the Commission needs to take into account the April 2018 e-evidence proposal, knowing that the latter may evolve during the legislative procedure. The Commission stressed on several occasions that an EU–US agreement can only be concluded following agreement on internal EU rules on e-evidence and adoption of the e-evidence regulation. In addition, the Commission has to comply with the mandate adopted by the Council, but also needs to consider the reactions of the Council and Member States within the Council during the negotiation phase.

Thus, the Commission is placed in an awkward position where it must be flexible enough to reach a compromise with US negotiators, but not so flexible as to allow the negotiations to be scrutinized by the Council, who has the power to sign the agreement. In the event of negotiations being blocked or necessitating a change in direction, the EU treaties allow the Council to adopt revised or new negotiating directives at any time during negotiations. This change can either be prompted by the Commission, which may seek to deviate from the previously agreed position, or it can result from a change in the position of the Member States.

The Parliament needs to be informed on an immediate and comprehensive basis at all stages of the procedure (Article 218(10) TFEU). Although the Parliament neither decides when the opening of negotiations takes place, nor defines the content of the negotiation directives, it gives its consent at the end of the negotiations (as this is a field where it acts as co-legislator). Therefore, the political support of the Parliament is strongly needed, and the Commission must report not only to the Council but also to the Parliament. The fact that e-evidence involves sensitive fundamental rights issues also explains the need for democratic control. Accordingly, the notes issued by the Commission at the end of the negotiation rounds are addressed to the two institutions.

The Parliament may signal its political position by issuing a resolution at any stage of the process. When this is done during the negotiations, it gives an idea of

73 Conclusions of the European Council of 18 October 2018. <https://www.consilium.europa.eu/en/press/press-releases/2018/10/18/20181018-european-council-conclusions/> accessed 10 October 2020.
74 Recommendation for a Council decision . . . (n 23).
75 'Commission hopes to launch negotiations on a transatlantic agreement on access to electronic evidence in June' (2019) Europe Daily Bulletin No 12232 Agence Europe.
76 See n 21.
77 Tom Delreux and Bart Kerremans, 'How Agents Weaken their Principals’ Incentives to Control: The Case of EU Negotiators and EU Member States in Multilateral Negotiations’ (2010) 32(4) Journal of European Integration.
78 cf n 20.
79 This is foreseen by rule 114 of the Parliament’s Rules of procedure, saying that: 'At any stage of the negotiations and from the end of the negotiations to the conclusion of the international agreement, Parliament may, on the basis of a report from the committee responsible, drawn up by that committee on its own initiative or after considering any relevant proposal tabled by a political group or Members reaching at least the low threshold, adopt recommendations to the Council, the Commission . . .
the way the Parliament wants the European negotiator to act.

The Parliament has been particularly active with regards to negotiations of similar agreements in the past, as in the case of the PNR agreements.80 So far, there is no EP’s resolution in relation to the EU–US negotiations on e-evidence, but some members of the Parliament (MEPs) have occasionally hinted that they intend to do so in the future. Where a resolution is adopted, the Commission is not legally bound to follow the recommendations of MEPs but given that the Parliament’s consent is required to adopt the agreement, it would be unwise to dismiss them. As a result, the Commission, when discussing this issue with the other party, must be attentive to the position of the two main EU institutions.

Conclusion of the agreement

When the negotiation comes to an end, the Council and the Parliament are informed, and the final text of the agreement is vetted by a group of lawyers from both institutions. This procedure is commonly referred to as ‘legal scrubbing’. This usually results in minor changes to the text. However, in the case of the Canada—EU Comprehensive Economic and Trade Agreement (CETA), new articles were added, and the highly controversial investor-state arbitration architecture was replaced by a new investment court system.

Once this legal stage is completed, the text is initiated (chief negotiators from each party place their initials on every page of the agreement to signify that the text has been agreed). Thereafter, the Council, in response to a proposal by the negotiator (here the Commission), firstly adopts a decision signing the agreement (Article 218(5) TFEU), and secondly a decision concluding the agreement (Article 218(5) TFEU). The voting rule under Article 218(8) TFEU is qualified majority. There are exceptions where the decision is made by unanimity, but none of these are applicable to the agreement on e-evidence. That means that 55 per cent of the 27 Member States (15 Member States) representing at least 65 per cent of the total population of the 27 Member States, need to vote in favour of the agreement.81

The powers of the Parliament with regards to the conclusion of international agreements have been considerably extended by the Treaty of Lisbon.82 In between the signing and the conclusion of the international agreement, the consent of the Parliament is needed in a number of scenarios, including ‘agreements covering fields to which either the ordinary legislative procedure applies, or the special legislative procedure where consent by the European Parliament is required’. Given that E-evidence is a topic about which the Parliament acts as co-legislator, obtaining the consent of the Parliament to conclude an external agreement with the US on the same matter is compulsory. Potentially, the Parliament has the power to obstruct the conclusion of the EU–US agreement. Yet, this power is not so easy to use. Indeed, as specified by the Parliament’s Rules of Procedure (Rule 114), when the Council requests that the Parliament give its consent to the conclusion, the Parliament shall decide by a single vote in accordance with Rule 105. No amendments to the text of the agreement shall be admissible. If the Parliament declines to give its consent, the President shall inform the Council that the agreement in question cannot be concluded. Refusing to give consent could have important consequences (ranging from additional delays to the impossibility of concluding the agreement), and is therefore rarely used by MEPs.

It should be recalled that the Parliament used this power in 2010 in relation to the TFTP Agreement.83 The Parliament was sceptical of this agreement and, in a Resolution adopted on 17 September 2009,84 reiterated its commitment to data protection and its desire to limit the scope of the agreement. It set out a series of conditions and expectations requesting from the Commission and the Council to strike a better ‘balance between security measures and the protection of civil liberties and fundamental rights, while ensuring the utmost respect for privacy and data protection’. Despite this, an interim TFTP Agreement was signed by the Council on 30 November 2009. Considering that this Agreement was far removed from what the Parliament had envisaged, and that it had no chance to amend it,

---

80 Juan Santos Vara and Soledad Sánchez-Tabernero (eds), ‘The Democratisation of EU International Relations Through EU Law’ (Routledge, London/New York 2018).
81 A voting calculator is available at <https://www.consilium.europa.eu/fr/council-eu/voting-system/voting-calculator/> accessed 10 October 2020.
82 Juan Santos Vara, ‘The Role of the European Parliament in the Conclusion of the Transatlantic Agreements on the Transfer of Personal Data after Lisbon’ CLEER Working Paper 2013/2.
83 The Parliament also refused to give its consent to the Second Protocol of the Fisheries Partnership Agreement between the EU and Morocco (2011) and to the Anti-Counterfeiting Trade Agreement (2012).
84 European Parliament Resolution P7_TA(2009)0016 of 17 September 2009 on the envisaged international agreement to make available to the US Treasury Department financial payment messaging data to prevent and combat terrorism and terrorist financing (2009) OJ CE224/8.
the Parliament rejected this Agreement on 11 February 2010 and requested a re-negotiation of the agreement. This led to an impasse and Member States criticized the European Parliament for jeopardizing European security. After a second negotiation period, some concessions were granted to the Parliament and the final TFTP Agreement was once again put to a vote on 8 July 2010 and was passed by the Parliament.

Commenting on the new powers of the European Parliament under the Lisbon Treaty, a scholar wrote that: ‘The growing influence of the EP, as well as its capacity to exert control over all stages of decision-making, has the potential to develop into a more stringent relationship where the European Parliament would be able to (informally) delegate tasks to the Commission – converting it into a (informal) principal.’ However, another scholarly contribution cast doubt on the idea that the European Parliament would be willing to play such an important role. It noted that, even in the TFTP case, the Parliament ‘ultimately gained few concessions from the United States and the Council in the second round of negotiations’ of the TFTP Agreement, ‘with their emphasis on security trumping most of the EP’s data protection concerns’. And it concluded that the European Parliament finally ‘abandoned its previous critical stances and is now becoming a new ‘norm taker’ within the EU-US relationship’.

The eventual role of the CJEU

In theory, the EU–US agreement on the LEA’s access to data can at least be—indirectly—subjected to careful scrutiny by the CJEU. Two hypotheses can be distinguished as to whether this control is a priori (before the agreement is concluded) or a posteriori (after the agreement is concluded).

The hypothesis of a priori control

According to Article 218(11) TFEU, a ‘Member State, the European Parliament, the Council or the Commission may obtain the opinion of the Court of Justice as to whether an agreement envisaged is compatible with the Treaties. Where the opinion of the Court is adverse, the agreement envisaged may not enter into force unless it is amended or the Treaties are revised’.

The purpose of the ex ante ‘constitutional control’ procedure, as regularly explained by the CJEU since Opinion 1/75, is to:

- fortiability complications which would result from legal disputes concerning the compatibility with the Treaty of international agreements binding upon the Community. In fact, a possible decision of the Court to the effect that such an agreement is, either by reason of its content or of the procedure adopted for its conclusion, incompatible with the provisions of the Treaty could not fail to provoke, not only in a Community context but also in that of international relations, serious difficulties and might give rise to adverse consequences for all interested parties, including third countries. For the purpose of avoiding such complications the Treaty had recourse to the exceptional procedure of a prior reference to the Court of Justice for the purpose of elucidating, before the conclusion of the agreement, whether the latter is compatible with the Treaty.

This procedure has not been widely used. Only 22 Opinions have been delivered in total until now. However, one third of this total has been delivered since 2010. The Opinion of the Court is often sought when the issue at stake is considered highly sensitive, such as the case of the CETA agreement (Opinion 1/1791) and the EU’s accession to the European Convention of Human Rights (Opinion 2/1392).

In the field of law enforcement-related treaties the most prominent example of such a priori control by the Court was Opinion 1/1593 on the draft agreement that addressed the Transfer of Passenger Name Record (PNR) data from the EU to Canada. In this Opinion

85 ‘SWIFT: European Parliament votes down agreement with the US’ (11 February 2010) Press release, European Parliament Justice and home affairs.
86 Ariadna Ripoll Servent and Alex MacKenzie, ‘The European Parliament as a ’Norm Taker’? EU–US Relations after the SWIFT Agreement’ (2012) 17 European Foreign Affairs Review.
87 Ariadna Ripoll Servent, ‘The Role of the European Parliament in International Negotiations after Lisbon’ (2014) 21(4) Journal of European Public Policy.
88 Servent and MacKenzie (n 86).
89 Servent and MacKenzie (n 86).
90 Opinion 1/75 of the Court of 11 November 1975 given pursuant to art 220 of the EEC Treaty, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61975CV0001> accessed 10 October 2020.
91 Opinion of the Court of 30 April 2019, Opinion 1/17, <http://curia.europa.eu/juris/document/document.jsf?&dir=&docid=213502&textid=&doclang=EN&part=1&occ=first&mode=DOC&pagelId=0&cid=750432> accessed 10 October 2020.
92 Opinion of the Court (Full Court) of 18 December 2014, Opinion 2/13, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CV0002> accessed 10 October 2020.
93 Opinion of the Court (Grand Chamber) of 26 July 2017, Opinion 1/15, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62015CV0001%2801%29> accessed 10 October 2020.
94 Christopher Kuner, ‘International Agreements, Data Protection, and EU Fundamental Rights on the International Stage: Opinion 1/15 (EU–Canada PNR) of the Court of Justice of the EU’ (2018) 3 Common
the CJEU tried to strike a balance between privacy and security. The Court considered surveillance as a necessary tool for the prevention of terrorism, but insisted that there should be very strict rules around the concrete implementation of such surveillance. Some of the draft agreement’s provisions were considered incompatible with Articles 7 (privacy) and 8 (data protection), read in conjunction with Article 52 (principle of proportionality) of the Charter of Fundamental Rights of the European Union. This made a renegotiation of the agreement necessary. Following this Opinion, the EU and Canada reopened negotiations on their PNR Agreement.95

Given that Article 218(11) is a procedure of a discretionary nature, it is far from certain that it will be used in relation to the EU–US Agreement on e-evidence. The most probable candidate to request such an Opinion would be the European Parliament, as occurred in Opinion 1/15. On the other hand, the Parliament did not use the procedure in relation to the EU–US Umbrella Agreement despite criticism of this Agreement by NGOs97 and even the EDPS.98 By the same token the Parliament did not request the opinion of the CJEU about the PNR agreement between the EU and Australia of 24 September 2011 and that with the US of 14 December 2011. In terms of the EU–US Agreement on e-evidence, a lot will depend on the content of the Agreement and on whether the Parliament considers that the Agreement is balanced enough and responds adequately to EU human rights requirements and safeguards. The Parliament’s Rules of procedure (Rule 114, point 6) specify the modalities of such a procedure. At any time before the Parliament gives its consent, the relevant Parliament Committee, or at least one-tenth of Parliament’s component members may propose that Parliament seeks an opinion from the Court of Justice on the compatibility of an international agreement with the Treaties.99 The Parliament’s resolution seeking an Opinion from the Court of Justice must then be adopted by a majority of the Parliament’s members.100

### The hypothesis of a posteriori control

Even if the Opinion of the Court is not demanded before the conclusion of the agreement, there is still the possibility of a posteriori control by the CJEU.101 Two main procedures could be used to challenge the agreement: ex-post action for annulment and preliminary references. In both cases, however, it is rather unlikely that the Court will invalidate an international agreement concluded by the European Union.

### Procedures: annulment and preliminary reference

The annulment procedure (Article 263 TFEU) is a direct action which guarantees conformity of EU secondary law (mainly regulations, directives, and decisions) with the superior rules contained in EU law. An action can be brought within two months of the publication or notification of the contested measure. Applicants are divided into three categories. Privileged applicants (Parliament, Commission, Council, Member States) do not have to prove that they have any particular interest in bringing a case before the Court. Non-privileged applicants, comprising all natural and legal persons, have to demonstrate that the contested act infringes upon their interests.

The preliminary reference procedure (Article 267 TFEU) is used when a national court or tribunal refers a question regarding EU law to the CJEU for a preliminary ruling so as to be able to decide on a case at Member State level. Here, the legal question is raised in a pending case before a court or tribunal of a Member State, and this court or tribunal brings the matter before the CJEU due to the fact that it may concern interpretation of the Treaties, or the validity and interpretation of acts of the institutions, bodies, offices or agencies of the Union. This procedure is said to be the cornerstone of EU law as it ensures uniform interpretation and validity of EU law across all Member States. Many of the Court of Justice’s landmark rulings have been issued as a result of a preliminary question, two of the most famous in

---

95 Arianna Vedaschi and Chiara Graziani, ‘PNR Agreements between Fundamental Rights and National Security: Opinion 1/15’ (European Law Blog, 23 January 2018) <https://europeanlawblog.eu/2018/01/23/pnr-agreements-between-fundamental-rights-and-national-security-opinion-115/> accessed 10 October 2020.

96 See Conclusions, point 6.

97 cf n 11.

98 EDPS (n 12).

99 Before Parliament votes on that proposal, the President may request the opinion of the committee responsible for legal affairs, which shall report its conclusions to Parliament. If Parliament approves the proposal to seek an opinion from the Court of Justice, the vote on a request for consent or opinion shall be adjourned until the Court has delivered its opinion.

100 On 25 November 2014, The European Parliament adopted by 383 votes to 271, with 47 abstentions, a resolution (Parliament Resolution 2016/C289/01 of 25 November 2014 seeking an opinion from the Court of Justice on the compatibility with the Treaties of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data (2014) OJ C289/2) tabled by the ALDE Group on seeking an opinion from the Court of Justice on the compatibility with the Treaties of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data (PNR).

101 Nadine Zipperle, EU International Agreements: An Analysis of Direct Effect and Judicial Review Pre- and Post-Lisbon (Springer, Cham 2017).
the field of data protection being the ‘Schrems I’ and the ‘Schrems II’ decisions.\(^\text{102}\)

The CJEU is said to be an audacious, and even an activist Court, which has contributed a great deal to the European integration process.\(^\text{103}\) In the field of data protection and privacy, judgments such as Tele2 Sverige AB and Watson\(^\text{104}\) of 21 December 2016, have been criticized by law enforcement agencies in Europe for going too far in prioritizing protection of rights\(^\text{105}\) over other competing interests, especially security.

The CJEU has already ruled on matters related to the conclusion and implementation of EU international agreements, and in theory could also do so in the case of the EU–US agreement on electronic evidence. Every time that the Court has argued that the CJEU has no jurisdiction to examine the validity of international agreements, the Court has persistently replied that it does indeed have jurisdiction, both in the context of an action for annulment and in the context of a request for a preliminary ruling, to assess whether an international agreement concluded by the EU is compatible with the Treaties and with the rules of international law which, in accordance with the Treaties, are binding on the Union. This was stated in Opinion 1/75 of 11 November 1975 and has since been regularly reaffirmed.\(^\text{106}\) The fact that international agreements concluded by the EU are binding not only on EU institutions, but also on third States that are parties to those agreements, is not enough to deny the Court’s jurisdiction. Indeed, when the Court has to rule on the validity of an international agreement concluded by the EU, this demand must be understood as relating to the EU act approving the conclusion of that international agreement.\(^\text{107}\) Thus, in accordance with the Court’s settled case law, international agreements concluded by the EU pursuant to the provisions of the Treaties, including a future EU–US agreement, constitute, as far as the Union is concerned, acts of EU institutions.\(^\text{108}\)

Judicial review of an external agreement is therefore possible under EU law. The CJEU could be asked whether the agreement on e-evidence complies with EU law and could proceed with the same type of control it exercised in its Opinion 1/15 on the PNR agreement with Canada, regarding the legal basis of the agreement and its compatibility with the EU Charter for fundamental rights.\(^\text{109}\)

However, is there a chance that one of the two procedures mentioned above will lead to the invalidation of a future EU–US agreement? Although this is not an impossible outcome it is, in our view, an unlikely one, for reasons related to international law, EU law and politics.

Consequences: an interpretative conciliation?

The prospect of an invalidation of a future EU–US agreement remains unlikely, for a series of reasons. Some of these are specific to each procedure; others are common to the two procedures.

The annulment procedure allows the CJEU to review the legality of EU legal acts—which may include the Council decisions to sign and conclude the agreement—on the grounds of lack of competence, infringement of an essential procedural requirement, infringement of the Treaties or any rule of law relating to their application, or misuse of powers.

A good example is the US PNR case which directly concerns a transatlantic law enforcement agreement, about the transfer of personal data by airlines to the USA.\(^\text{110}\) In the case of Parliament v Council (C-317/04, judgment of the Court (Grand Chamber), 30 May 2006), the Court of justice annulled Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the US on the processing and transfer of PNR data by air carriers to the US authorities. But at that time, there was no obligation to obtain the Parliament’s consent. Only an opinion of the Parliament was required. Interestingly, the Parliament did not ask for an a priori control/Opinion of the Court before the conclusion of the agreement (an Opinion was initially requested but was withdrawn in the end by the Parliament). But this did not prevent the Parliament seeking annulment of the Council’s decision on the EU–US PNR Agreement.

However, where the EU–US agreement on e-evidence is concerned, the likelihood of an annulment action is low because most of the so-called privileged applicants are now part of the treaty-making process: the Council

102 Case C-362/14, Maximilian Schrems v Data Protection Commissioner (2015). See n 317 and Post Scriptum on Schrems II.
103 Sabine Saurugger and Fabien Terpan, The Court of Justice of the European Union and the Politics of Law (European Union Series, Palgrave McMillan, Basingstoke 2017).
104 Joined Cases C-203/15 and 698/15 Tele2 Sverige AB and Watson [2016].
105 Orla Lynskey, ‘Tele2 Sverige AB and Watson et al: Continuity and Radical Change’ (European Law Blog, 12 January 2017) <https://europeanlawblog.eu/2017/01/12/tele2-sverige-ab-and-watson-et-al-continuity-and-radical-change/> accessed 10 October 2020.
106 For instance: Case C-327/91 France v Commission [1994]. And for a recent example: Case C-266/16 Western Sahara Campaign UK [2018].
107 The US Supreme Court, by contrast, does not review international agreements against the requirements of the US Constitution, because it considers them ‘political questions’ entrusted to the Executive branch.
108 Case C-162/96 Rache [1998], para 41, and Case C-386/08 Brita [2010], para 39.
109 See Kuner (n 94).
110 Joined Cases C-317/04 Parliament v Commission and C-318/04 Parliament v Council [2006].
adopts the decisions signing and concluding the agreement; the Commission, as the negotiator, finalizes the last version of the agreement; the Parliament gives its consent.\textsuperscript{111} It would be highly unlikely for these actors to consent to the conclusion of the agreement and then challenge its validity in front of the CJEU. This is especially the case as they are able to request a preliminary opinion from the Court before the agreement enters into force, if they have any doubt about its conformity with EU law.

Non-privileged applicants—natural and legal persons—may also institute proceedings but only if they meet certain conditions. An action can firstly be brought against an act addressed to that person or which is of direct and individual concern to them. A litigant should not be directly and individually concerned by a decision concluding an agreement, but he or she could meet this condition in the case of a decision based on the EU–US agreement. Secondly, the action can be brought against a regulatory act which is of direct concern to them and does not entail implementing measures. Assuming that a decision concluding an agreement is considered a regulatory act, the condition of ‘direct concern’ would still have to be met. The CJEU usually applies this condition quite restrictively, particularly where NGOs are concerned.\textsuperscript{112} For example, in its Order of 22 November 2017,\textsuperscript{113} the General Court (second chamber) of the CJEU ruled that an action brought by Digital Rights Ireland (DRI) against the Commission’s Privacy Shield decision, on behalf of DRI, its members, its supporters and the general public, could not be found admissible. DRI could not prove it had an interest in bringing proceedings. And EU law does not, in principle, allow for the possibility of an applicant bringing an actio popularis in the public interest. However, depending on the circumstances, it is not impossible for an NGO to demonstrate that it is ‘directly concerned’ as the result of a regulatory act.\textsuperscript{114}

Apart from the annulment procedure, a preliminary reference could also question the validity of an EU–US data access agreement. When the time period within which the annulment action can be brought before the Court has elapsed, the preliminary reference might be a solution that could be perceived as a last resort. For private parties, it might also be the only realistic solution, considering how difficult access is to the annulment procedure. A recent example of a preliminary ruling concerning an international agreement is that of the Western Sahara Campaign UK,\textsuperscript{115} in which the Court assessed the validity of Council decisions about the conclusion of the fisheries partnership agreement between the European Community and Morocco, in response to a request for a preliminary reference from two different courts in the UK. The case at domestic level involved an NGO whose aim is to support the recognition of the rights of Western Saharan people to self-determination. More generally, NGOs and other private parties use litigation strategies to get the CJEU to invalidate an EU act. Such strategies could also be used with the EU–US agreement on e-evidence.

Comparisons could also be made with the famous ‘Schrems’ cases. In ‘Schrems I’, issued on 6 October 2015, the Court invalidated the Safe Harbour arrangement for cross border data transfers between the EU and the US.\textsuperscript{116} In ‘Schrems II’, issued on 16 July 2020, the Court invalidated the Privacy Shield arrangement, which was the successor to Safe Harbour, and also advised that data controllers must ‘verify whether the law of the third country of destination ensures adequate protection under EU law’\textsuperscript{117} when they use Standard Contractual Clauses for data transfers. Both Schrems I and II were brought to the CJEU through the preliminary reference procedure. However, these comparisons

\textsuperscript{111} Member State, and more specifically a Member State who voted against the Council decisions, could also start a procedure.

\textsuperscript{112} This is an important issue as NGOs are making increasing use of litigation strategies for data protection purposes. See for instance the role played by Digital Rights Ireland in the invalidation of the Data Retention Directive. MP Granger and K Irion, ‘The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling off the EU Legislator and Teaching a Lesson in Privacy and Data Protection’ (2014) 39(4) European Law Review 835–50.

\textsuperscript{113} Case T670/16 Digital Rights Ireland Ltd v European Commission – Order of the General Court [2017].

\textsuperscript{114} In T-738/16, French privacy NGOs La Quadrature du Net, French Data Network, Fédération des Fournisseurs d’Accès à Internet Associatifs (F- FIDM) brought an action for annulment before the General Court against the Commission adequacy decision on the Privacy Shield regime. The action has not been found inadmissible, but this issue was supposed to be joined with the substance of the case. Bearing in mind that the CJEU invalidated Privacy Shield in Schrems II, the Court might now dismiss the case as moot.

\textsuperscript{115} Case C-266/16 Western Sahara Campaign UK [2018].

\textsuperscript{116} Case C-362/14 Maximillian Schrems v Data Protection Commissioner (Schrems I) [2015]. The ruling involved a privacy activist, Maximilian Schrems, who took action at national level. Maximilian Schrems filed an application for judicial review to the Irish High Court in response to the inaction of the Irish Data Protection Commissioner, invoking both Directive 1995/46/EC and arts 7 and 8 of the European Charter of Fundamental Rights (on respect for private life and the protection of personal data respectively). The High Court appealed to the CJEU, questioning the Commission’s adequacy decisions and asserting that Safe Harbour ensures an adequate level of protection with respect to the data of European citizens when transferred to the USA. The CJEU ruling invalidated the Commission Decision, leading EU and US authorities to find a new arrangement, the so-called Privacy Shield, which was in its turn invalidated by the CJEU in July 2020.

\textsuperscript{117} Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems [2020], para 134. For a brief discussion see the Post-Scriptum.
have limitations. The two Schrems cases did not challenge any international agreement between the EU and the US. They exclusively challenged an EU Commission decision stating that US law—as reflected in political declarations made by US authorities and included in the Safe Harbour package—ensured a sufficient level of protection in relation to the data of European citizens when transferred to the USA. This, of course, is of fundamental importance for cross border data transfers and has extremely important practical consequences.\(^\text{118}\)

However, although the annulment of the Commission decisions leads to the European Court giving a legal assessment of a foreign law, this is not a problem from an international law point of view.

On the contrary, a future ‘invalidation’ of an EU–US Agreement on e-evidence by the Court could raise important issues of international law, as the agreement will be a proper binding international commitment.\(^\text{119}\)

Indeed, in application of the customary rule codified by the Vienna Convention of 21 March 1986 on the law of treaties between States and International Organizations, an ‘international organization party to a treaty may not invoke the rules of the organization as justification for its failure to perform the treaty’.\(^\text{120}\)

Similarly, the international law of treaties does not authorize the EU to invoke EU rules (for instance the EU Charter of Fundamental Rights) as a means of challenging the validity of an international agreement.\(^\text{121}\)

This means that, should the CJEU ‘invalidate’ the decision to conclude an international agreement, the EU could be held accountable under international law and engage its international responsibility.\(^\text{122}\)

In reality, any eventual ‘annulment’ of such a decision by the CJEU can only be framed as an ‘order’ for the EU to denounce/withdraw from the international agreement. Such a denunciation can in no way have retroactive effects with regard to international law. This means that an annulment of a decision concluding an international agreement could only lead to a termination of the treaty taking effect ex nunc; in no way could this lead to a retroactive ‘invalidation’ of the international agreement.

Apart from purely legal arguments, operational considerations (the negative effects of transatlantic law enforcement cooperation) as well as international politics seem to command the highest cautiousness. The EU, one of the most continuous supporters of multilateralism and international law, strives to promote a rules-based international system and to show it complies with international law.

Admittedly there are famous examples of the Court being less cautious and deciding that EU law should prevail over the EU’s international commitments. In the case of Kadi, the Court applied a dualist approach often ‘described as unfaithful to its traditional fidelity to public international law’\(^\text{123}\) and gave precedence to EU law over a United Nations Security Council (UNSC) resolution, adding that it could be different in the future if adequate human rights safeguards were introduced at international level. This created a lot of controversy between the EU and international lawyers.\(^\text{124}\)

In the case of France v Commission (C-327/91), the Court declared that a decision of the Commission to conclude an agreement with the US about competition was void, on the grounds that the Commission was not competent. In other cases, the Court made it clear that, if an international agreement is concluded in breach of the duty of sincere cooperation, it can be denied effect in the EU legal order.\(^\text{125}\)

And in Germany v Council (C-122/95), the Court annulled the Council decision concerning the another body that the Council (with the consent of the Parliament) pretend having concluded an international agreement, which is rather inconceivable.

\(^{118}\) The strong—not to say somehow apocalyptic—titles by the Press following these two judgments illustrate the fundamental impact of the rulings of the CJEU. See for instance after Schrems II: Vincent Manancourt, ‘The Demise of Privacy Shield may be the End of US–Europe Data Transfers’ (Politico, 3 August 2020, <https://www.politico.eu/article/privacy-shield-is-dead-long-live-data-localization/> accessed 10 October 2020).

\(^{119}\) Enzo Cannizzaro, Paolo Palchetti and Ramses A Wessel (eds), International law as law of the European Union (Martinus Nijhoff Publishers, Leiden 2011).

\(^{120}\) Art 27.

\(^{121}\) The only exception to this rule is the exceptional hypothesis of ‘imperfect ratifications’ envisioned by art 46(2) of the Vienna Convention, which could not apply here anyway. This article provides that ‘An international organization may not invoke the fact that its consent to be bound by a treaty has been expressed in violation of the rules of the organization regarding competence to conclude treaties as invalidating its consent unless that violation was manifest and concerned a rule of fundamental importance’ (art 46-2). Such a violation is manifest ‘if it would be objectively evident to any State or any international organization conducting itself in the matter in accordance with the normal practice of States and, where appropriate, of international organizations and in good faith’ (art 46-3). This means that such an exception could apply to the EU only if . . .
conclusion of the World Trade Organisation (WTO) Agreement to the extent that it approved the Framework Agreement on Bananas, arguing that provisions of that Framework Agreement infringed a general principle of Community law: the principle of non-discrimination. Advocate-General Maduro argued in his Opinion delivered in the Case of Kadi:

All these cases have in common that, although the Court takes great care to respect the obligations that are incumbent on the Community by virtue of international law, it seeks, first and foremost, to preserve the constitutional framework created by the Treaty. Thus, it would be wrong to conclude that, once the Community is bound by a rule of international law, the Community Courts must bow to that rule with complete acquiescence and apply it unconditionally in the Community legal order. The relationship between international law and the Community legal order is governed by the Community legal order itself, and international law can permeate that legal order only under the conditions set by the constitutional principles of the Community.126

However, cases where the Court has questioned an EU international agreement remain relatively rare. The Court will reasonably seek to avoid such situations as they are highly controversial and can potentially have important and unwelcome consequences: legally, because they challenge international law and the EU’s international commitments; and also politically because the Court challenges the balance of power that most of the times has led, throughout a long process of negotiation, to a fragile and difficult compromise.

This is the reason why, if the Court finds during an ‘a posteriori’ control scenario that there is an incompatibility with EU law problem in an international agreement concluded by the EU, it will most probably try to effect what we could call an ‘interpretative conciliation’ (or ‘conciliatory interpretation’) between the two.

This is perfectly illustrated by some recent CJEU judgments concerning Western Sahara. In two different set of cases, applicants challenged the validity of a series of international agreements concluded between the EU and Morocco,127 based on the argument that these agreements included products and goods emanating from Western Sahara (ruled, for the most part, illegally by Morocco according to the applicants) which thus violated the fundamental principle of self-determination of peoples binding upon the EU. Instead of invalidating all these agreements, the CJEU interpreted them in a way that was compatible with International/EU Law by limiting their territorial scope: the CJEU ruled that all these agreements must be interpreted as not covering Western Sahara—and thus rejected the applications as inadmissible.128

This strategy of ‘interpretative conciliation’ between international agreements and EU rules (or, where Western Sahara is concerned, international rules binding upon EU and being part of EU law) is very effective but has an important limitation: the interpretation proposed by the CJEU must also be accepted by the other party to the international agreement. It takes two to tango! Assume, for instance, that tomorrow the EU and the US conclude an agreement on electronic evidence, an applicant (like Schrems!) succeeds in one way or another at challenging such an agreement in a national Court and the case finally arrives at the CJEU though the preliminary reference procedure. Assume also that the CJEU then conducts an important ‘interpretative conciliation’ in order to interpret the EU–US Agreement in a way that is compatible with EU law. Depending on the importance of the ‘interpretation’ proposed by the Court and its effects on the US, the US could either accept it (in which case the Agreement would henceforth be interpreted in the way suggested by the CJEU) or disagree with it, in which case the EU and the US would need to negotiate in order to find a solution.

Conclusions

Seven main conclusions can be drawn from the previous analysis:

1. There are three possible options for the architecture of a transatlantic agreement on cross-border access to electronic evidence for judicial cooperation in criminal matters.

The first option is the conclusion of a single, comprehensive and self-standing EU–US Agreement (the ‘PNR’ or ‘TFTP’ model). This is the preferable option for the EU and, without doubt, the quickest, at least from the point of view of European Law. However, this option raises a lot of difficulties for the US and there is a lot of uncertainty as to whether the CLOUD Act can authorize the conclusion of an agreement with the EU only. This means that such a self-standing EU–US Agreement might need to be concluded outside the CLOUD Act framework.

126 Opinion of Advocate General Poiares Maduro delivered on 23 January 2008, Case C415/05 P, Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities.

127 Specifically, the EU–Morocco Association Agreement, the Liberalisation Agreement and the EU–Morocco Fisheries Partnership Agreement.

128 See Case C-104/16 P Council v Front Polisario [2016] and Case C-266/16 Western Sahara Campaign UK [2018].
(which could create delays and require qualified majorities in the US Congress).

The second option is to conclude an EU–US framework agreement followed by bilateral agreements between the US and EU Member States. This is the ‘MLA’ or ‘Extradition’ model. Such a solution could be preferable for the US but raises political difficulties for the EU as it could lead to unequal treatment among EU countries. Moreover, the process of concluding all these agreements could be time-consuming. It took 8 years for the MLA/Extradition agreements to enter into force. Can transatlantic cooperation on cross-border access to electronic evidence wait this long? What would the consequences be for LEAs and service providers of the numerous conflicts of laws persisting over this period? Is there a way to ‘speed up’ the process?

A third, theoretical option, is to transform the projected agreement into a ‘mixed agreement’ at a later stage. Such an option could satisfy the formal requirement of the CLOUD Act to conclude an executive agreement with ‘foreign governments’. However, it raises a lot of legal, institutional and other difficulties for the EU and does not seem to present any kind of benefit in relation to the specific expectations of the two sides. For instance, based on precedents, such an option would not allow the US any ‘unilateral certification’ power to ‘pick and choose’ which EU Member States are allowed to join the agreement.

2. The EU rules on competence indicate that EU Member States cannot negotiate and, most definitely cannot conclude bilateral agreements with the US during the period of EU–US negotiations. Doing so could expose them to an infringement procedure. Following the adoption of the EU–US Agreement the conclusion of bilateral US/Member State agreements can only be possible to the extent authorized by the EU–US Agreement.

3. Whatever the architecture/option chosen for the EU–US Agreement, it must be emphasized that the EU cannot conclude an ‘executive’ agreement as such. An executive agreement is a ‘treaty that has been concluded and ratified by the executive branch without formal approval by a legislative body, in a State in which treaties are usually ratified only with such approval. The term executive agreement refers only to the status of the agreement within the domestic law of the State in question’.129 If we consider that in the EU the ‘executive branch’ is the Commission, then it must be underlined that the Commission can initiate and negotiate international agreements but has no power to conclude them.130 As explained in the section ‘Adoption of international agreements by the EU: a multi-stage/multiactor process’, the adoption of an EU external agreement is a complicated process involving the Commission, the Council, and the Parliament. The European Parliament would need to consent to the conclusion of the EU–US Agreement.

4. This EU method of concluding agreements is, nonetheless, consistent with having the US agree via an executive agreement. Indeed, it is perfectly possible to conclude the agreement in different ways according to which side of the Atlantic you are on. The UK–US Agreement, for instance, was concluded using different procedures. The UK’s domestic approval procedure is ratification by Parliament.131 The US counterpart procedure, specified in the CLOUD Act itself, is for the executive to submit the agreement to Congress for a 180-day period of review; if neither house of Congress objects during that time period, the agreement is permitted to enter into force.132 Similarly, previous EU–US law enforcement agreements have followed different domestic approval procedures.

5. The fact that the European Parliament needs to consent to an EU–US e-evidence Agreement, raises the question of its influence (and eventual veto power). Past precedents (especially the TFTP Agreement) show that the Parliament might use this power in order to set conditions for giving consent. While the Parliament has not yet adopted any resolution in relation to the ongoing EU–US negotiations, some MEPs have emphasized that the Parliament will exercise diligence with regard to the introduction of important fundamental rights protections and other safeguards and conditions in the Agreement. Some have also requested the opinion of the EDPB about this.133 However, past experience also shows that the Parliament is pragmatic and understands that the

129 Christakis and Propp (n 16).
130 There is one area—the Common Foreign and Security Policy—where the Council can be seen as the ‘executive branch’ and can conclude an agreement alone, but this is not relevant here.
131 Explanatory Memorandum to the Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, UK Command Paper No 178, Policy Consideration (v).
132 CLOUD Act, above s 105 (adding 18 USC s 2523).
133 See EDPB Letter (n 29).
Commission must tread a thin line between taking into consideration the cumulative (but eventually divergent) expectations of the Council and Parliament while also finding a mutually satisfactory compromise with US negotiators. In the past, temporary objections or even rejections by the European Parliament have resulted in relatively quick solutions. And there is no precedent whatsoever for an EU–US law enforcement agreement project that has failed because of Parliament opposition.

6. Following the end of the negotiations and prior to the conclusion of the agreement, a Member State, the European Parliament, the Council or the Commission may request the opinion of the CJEU as to whether the agreement envisaged, but not yet in force, is compatible with the Treaties. The most probable candidate to do so would be the European Parliament, as it did with the EU–Canada PNR Agreement. However, the Parliament does not systematically request such opinions. For instance, the European Parliament did not request such an opinion with respect to the EU–US Umbrella Agreement despite some criticism of this Agreement, including criticism from the EDPS.

In any case, taking into consideration this eventual- ity, the EU and the US have an interest in working hard on the projected transatlantic Agreement on e-evidence to make it Court-proof. In the case of the PNR Agreement with Canada, the procedure was considerably delayed by the Court’s Opinion which stated that the Council’s decision on the conclusion of the agreement did not comply with EU law. While the negotiating mandate was adopted on 2 December 2010 and the envisaged agreement was initialled on 6 May 2013, the Opinion issued in July 2017 triggered a renegotiation of the agreement between December 2017 (new authorization given by the Council to the Commission) and July 2019 (EU–Canada summit acknowledging the conclusion of the negotiation phase).

The duration of the procedure has more than doubled due to the Court’s intervention. It would be detrimental to the interests of law enforcement agencies but also service providers in the EU and the US to have such huge delays in view of the eagerly expected EU/US Agreement (which intends, among other things, to resolve conflicts of laws).

7. After the EU–US Agreement enters into force, there still persists a theoretical possibility of a posteriori control by the CJEU, either through the annulment or preliminary references procedures. An NGO or private party could challenge the agreement either directly through an action for annulment, provided that the Court finds the action admissible, which is not a frequent occurrence where non-privileged applicants are concerned, or indirectly through preliminary references, which is more likely. However, an ‘invalidation’ of the EU–US Agreement after its entry into force would be improbable. This would not only create major political and operational difficulties for all stakeholders but would also raise serious issues of international law: the EU cannot in principle challenge the validity of an international agreement on the basis of an eventual incompatibility with EU law. In order to invalidate an external agreement while complying with the principles of international law, the CJEU could render a negative judgement requesting that the EU Council proceed to a denunciation/termination of the agreement which would only produce its effects ex nunc, not ex tunc. Landmark rulings like Kadi have shown that the CJEU might sometimes give precedence to EU law over international law, and is keen to preserve the autonomy of the EU legal order. However, previous case law (such as the ‘Western Sahara’ cases) shows that the CJEU, without challenging the validity of an international agreement concluded by the EU, could try to proceed to an ‘interpretative conciliation’ with EU law. If such a scenario materializes, it remains to be seen whether the US will accept the interpretation proposed by the Court (in which case the agreement would be automatically ‘modified’ in an informal way in accordance with the common will of the contracting parties) or challenge it, in which case a renegotiation might be necessary.

**Post-scriptum: the effects of the Schrems II CJEU judgment**

Following the submission of this article, on 16 July 2020 the CJEU issued an extremely important judgment in the Schrems II case invalidating the Privacy Shield arrangement and affirming strongly the importance of maintaining a high level of personal data protection when transferred from the European Union to third countries.134 This ‘constitutional’ judgment has since been analysed in a great number of articles.135 We

134 See n 117.
135 See inter alia: Christopher Kuner, ‘The Schrems II Judgment of the Court of Justice and the Future of Data Transfer Regulation’ (European Law Blog, 17 July 2020, <https://europeanlawblog.eu/2020/07/17/the-
will only make a few brief observations here about whether and how Schrems II might affect the ongoing negotiations between the EU and the US on LEA access to data.

Let’s start by emphasizing once again the differences between the content of the ongoing EU–US negotiations at the heart of this article and the subject matter in Schrems II. The former is about LEA access to data held by service providers with regard to criminal investigations and regardless of the place where the data is located; the latter is about the conditions upon which international transfers of data can occur for commercial purposes—and especially the protections against government (and especially intelligence agencies’) access to data already transferred by a company to another jurisdiction.  

From a formal point of view, in the first case the EU and the US are trying to conclude a binding agreement under International Law; in the second case no international treaty was at stake: the CJEU invalidated an internal act of the EU (Commission Decision 2016/1250 that was the legal basis of the EU–US Privacy Shield arrangement), albeit one that has important international consequences.  

That being said, one should also highlight the potential convergence between the two issues. Indeed, in both cases what is at stake after all is government access to data and the safeguards and remedies that should be introduced in the legal regime. In both cases the challenge is to find the right balance between the need for expedient access to information by government agents (law enforcement and/or intelligence agencies) and the need for a sufficiently high level of privacy and data protection, including effective judicial remedies.

From a formal point of view, while both the Safe Harbour and the Privacy Shield arrangements took the form of an ‘adequacy decision’ by the Commission, nothing in theory prohibits the conclusion of an international binding agreement between the EU and the US on these issues. Indeed, as mentioned earlier, some authors, who have been highly critical of the invalidation of these two arrangements by the CJEU, blamed the outcome on the fact that the US was unable to obtain a ‘binding assurance’ from the EU about these issues and considered that the only solution for the US would be to conclude a ‘binding international agreement’ with the EU in the future.

In theory, then, a possible scenario could be to broaden the EU/US e-evidence and CLOUD Act discussions in order to include a Schrems ‘solution’, providing for a comprehensive and all-inclusive international treaty on government access to data and cross-border data transfers.

Such a scenario, however, would complicate the already highly complex and challenging ongoing negotiations on law enforcement access to data even further. History has shown that even relatively modestly scaled agreements that the EU and US have negotiated about this range of issues over the years (PNR, SWIFT, Umbrella, not to mention the Safe Harbor/Privacy Shield arrangements...) have been enormously difficult and time-consuming. Furthermore, taking into consideration that, in any case, a solution to the problems highlighted by the CJEU in Schrems II will require modifications to US law (on issues such as judicial redress or proportionality) one could expect that linking the two issues could lead to an extremely time-consuming process and a particularly thorny negotiation. Pending the conclusion of such an all-inclusive treaty, the post-Schrems II legal uncertainties on data transfers to the US would persist, as would the potential conflicts of law issues discussed in this article.

It might therefore not be practical nor in the interests of transatlantic cross border data flows and law enforcement cooperation to link the two issues. It might be better for the two negotiation processes to remain in parallel but distinct from each other. It remains to be seen, however, if and how the one process could influence the other and whether the negotiating parties might be tempted to leverage their strength into one of the negotiation blocks in order to obtain concessions...
from the other side in the other block. One thing is sure, the upcoming years will be a highly interesting period for the negotiation of transatlantic cross border data arrangements.

Post-scriptum 2: The effects of the October 2020 data retention/collection judgments

On 6 October 2020 the CJEU issued another series of very important judgments concerning government access to communication (traffic, location, subscriber) data. Three of these judgments were related to national legislation in France and Belgium requiring providers of electronic communications to undertake data retention in the interests of combatting crime and safeguarding national security, while the fourth judgment was related to UK legislation compelling providers to deliver bulk communications data directly to UK intelligence agencies. These judgments (hereafter: ‘2020 data retention/collection judgments’) are extremely complex and require detailed study. We will limit ourselves here, once again, to two series of thoughts on what their impact could be in relation to the subject matter of this article.

First, there is an aspect of these judgments that could eventually support the transatlantic dynamic of negotiating agreements on governments’ access to data by showing that the Court will hold EU Member States to standards analogous to the ones it has applied to the US in the Schrems I and Schrems II cases. More specifically, in the 2020 data retention/collection judgments, the CJEU rejected the arguments advanced during the proceedings by France and the UK, which were supported by a number of other EU Member States intervening in their favour, that the EU should decline its jurisdiction because the data retention/collection laws at stake were related to national security and thus fell under the exception provided by Article 4(2) of the TEU and Article 1(3) of the ePrivacy Directive. The Court held that, while these exemptions remained relevant in other cases (for instance when intelligence agencies process data themselves), they do not apply when State authorities make requests to service providers who process data. This means that EU Member States can only make such requests to service providers on the basis of the derogation of Article 15(1) of the ePrivacy Directive and means that they are bound by all EU law requirements and safeguards when they do so, notwithstanding the fact that their requests are motivated by national security considerations.

This position of the Court could in theory have a beneficial effect on transatlantic relations. The Court has been accused in the past of dealing with foreign countries’ surveillance laws (in the Schrems I and Schrems II cases) while being unable to exercise jurisdiction over Member States’ surveillance laws because of the ‘national security’ exemption. This argument was debatable, even before the 2020 data retention/collection judgments, as the Court had already restricted the room for manoeuvre of the Member States and the extent of the “national security” exemption; it is not valid anymore when taking into account the new judgments. By affirming that the same protective regime applies to EU Member States and foreign countries within the “adequacy” assessment decisions, the Court is able to dismiss the accusation of applying ‘double standards’. This could, in turn (and always theoretically), compel the EU and the US to work together towards the conclusion of transatlantic instruments related to the necessary standards that should govern States’ authorities access to data, both in the intelligence agencies field and in the law enforcement field.

A second thought, related to the first reflection, is that the CJEU explains, via the 2020 data retention/collection judgments, what kind of safeguards countries should apply when they make requests to service providers. These include prior authorization requirements, necessity and proportionality considerations or when and how notice to users should be given. All these considerations should be taken into account when drafting

141 Judgments in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others.
142 According to which: ‘The Union shall respect the ... essential State functions [of Member States], including ... national security. In particular, national security remains the sole responsibility of each Member State’.
143 According to which: ‘This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, ... and in any case to activities concerning public security, defence, State security ...’.
144 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
145 According to which: ‘Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in [this directive] ... when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences ...’.
146 This argument was raised, once again, in the recent US Department of Commerce/Department of Justice, White Paper, ‘Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II’, September 2020. See p 15 (‘The EU itself has no competence over national security matters, which are the sole responsibility of the EU Member States’) or p 18 (affirming that the CJEU ‘may not have jurisdiction’ to rule on issues related to national security ‘given restrictions in the EU treaties’).
147 cf Case C-203/15, Tele2 Sverige (n 104), para 72–73.
the EU–US agreement about LEAs access to data, so as to make it Court-proof. The present article was not intended to discuss the numerous, important and challenging issues of *substance* in the EU–US negotiations; but we do hope to be able to analyse all these issues and the precise relevance of the 2020 data retention/collection judgments in a subsequent study.

**Acknowledgement**

We would like to express our gratitude to all the colleagues who contributed useful comments on previous versions of this article: Karine Bannelier, Paul James Cardwell, Elaine Fahey, Kenneth Propp, Peter Swire, Juan Santos Vara, Ramses Wessel. We would also like to warmly thank warmly the members of the European Commission’s Negotiating Team Peter-Jozsef Csonka, Mark-Stephen Gray and Tania Schroeter for their helpful comments and insights. We would finally like to thank the anonymous reviewers of the International Data Privacy Law as well as the Editors for their very useful comments and for permitting to improve and update enabling the improvement and updating of the article. All errors are ours. This article covers developments till the 17th June 2020. The two post-scriptum cover developments till the 6th October 2020.

*doi:10.1093/idpl/ipaa022*