Douwe Korff
Emeritus Professor of International Law, London Metropolitan University
Associate, Oxford Martin School, University of Oxford

Ian Brown
Visiting CyberBRICS professor at
Fundação Getulio Vargas (FGV) Law School
in Rio de Janeiro

SOME BRIEF INITIAL COMMENTS ON
The announcement of an "agreement in principle" on a new Trans-Atlantic Data Privacy Framework & on the EDPB's statement on the agreement in principle

1. Background[1]

EU data protection law only allows free transfers of personal data to a non-EU country (a so-called "third country") if the third country in question provides "adequate" protection to the transferred data – and in its *Schrems I* judgment, the Court of Justice of the EU (CJEU) has held that this means that the third country must provide "essentially equivalent" protection to the EU rules, more specifically in relation to commercial data, to the EU General Data Protection Regulation (GDPR). One element of "adequacy" is that the third country in question must not grant its authorities excessive powers to access the transferred data.

In general terms, a third country's laws can only be said to provide such protection if they meet the standards set out in the European Data Protection Board (EDPB) Adequacy Referential. And in relation to access to personal data by a third country's intelligence agencies, its laws can only be said to provide this protection if they meet the standards set out in the EDPB's European Essential Guarantees for surveillance. Both documents fully reflect the CJEU's case law.

Because US surveillance law was held not to meet those standards, two previous adequacy decisions, under which US companies could self-certify compliance with rules broadly reflecting the EU standards – the EU-US Safe Harbour Agreement and its successor, the Privacy Shield – were declared invalid by the CJEU (in, respectively, its *Schrems I* and *Schrems II* judgments). The two main issues that led to these judgments were the powers of access to data by US authorities, in particular its intelligence agencies acting under the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333, as applied under Presidential Policy Directive 28 (PPD-28), which the Court found were not limited to what is necessary and proportionate to the (in itself of course legitimate) aim of protecting national security, and the lack of effective judicial redress by (and standing of) individuals from the EU in relation to such undue access.

Since the *Schrems II* judgment, there have been intensive discussions between the EU and the US on how to resolve the issues and come up with a new legal arrangement for EU-US data transfers that would meet the EU treaties', Charter of Fundamental Rights and GDPR requirements.

In the study commissioned by the European Parliament's Civil Liberties Committee (LIBE) last year, we concluded that there were serious obstacles to such an arrangement. In particular, in order to meet the EU treaties' and CFR requirements, the US will have to reform its surveillance laws in terms of both its substance an as concerns individual remedies and standing – and if a new arrangement were to still be based on a system of self-certification, that system would have to be fundamentally different from the earlier one, with greater powers for the Federal Trade Commission (FTC). (See further at 4, below.)

---

[1] For details and references, see Ian Brown & Douwe Korff, Exchanges of personal data after the Schrems II judgment, study carried out at the request of the European Parliament's Civil Liberties (LIBE) Committee into the future of EU – US flows of personal data, July 2021, sections 1.1, *Background*, and 2.3, *Implications for data transfers*: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf

2. The agreement in principle

On 25 March, the European Commission and the US Government made coordinated announcements that:[2]

> they have agreed in principle on a new Trans-Atlantic Data Privacy Framework, which will foster trans-Atlantic data flows and address the concerns raised by the Court of Justice of the European Union in the Schrems II decision of July 2020.

The statement said that the US side would:

> implement reforms that will strengthen the privacy and civil liberties protections applicable to U.S. signals intelligence activities. Under the Trans-Atlantic Data Privacy Framework, the United States is to put in place new safeguards to ensure that signals surveillance activities are necessary and proportionate in the pursuit of defined national security objectives, establish a two-level independent redress mechanism with binding authority to direct remedial measures, and enhance rigorous and layered oversight of signals intelligence activities to ensure compliance with limitations on surveillance activities.

And that:

> The teams of the U.S. Government and the European Commission will now continue their cooperation with a view to translate this arrangement into legal documents that will need to be adopted on both sides to put in place this new Trans-Atlantic Data Privacy Framework. For that purpose, these U.S. commitments will be included in an Executive Order that will form the basis of the Commission's assessment in its future adequacy decision.

3. The EDPB statement on the announcement of the agreement in principle

On 6 April 2022, the European Data Protection Board (EDPB) welcomed the announcement of what it referred to as a "poltical agreement in principle",[3] It felt that:

> The commitment of the U.S. highest authorities to establish 'unprecedented' measures to protect the privacy and personal data of individuals in the European Economic Area (EEA individuals) when their data are transferred to the U.S. is a positive first step in the right direction.

However, it stressed that:

> [The in-principle announcement] does not constitute a legal framework on which data exporters can base their data transfers to the United States. Data exporters must therefore continue taking the actions required to comply with the case law of the CJEU, and in particular its Schrems II decision of 16 July 2020.

Moreover:

---

[2] European Commission, *European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework*, 25 March 2022, available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087

[3] EDPB, Statement 01/2022, available at: https://edpb.europa.eu/system/files/2022-04/edpb_statement_202201_new_trans-atlantic_data_privacy_framework_en.pdf

> The GDPR requires that the Commission seeks an opinion of the EDPB before adopting a possible new adequacy decision recognising as satisfactory the level of data protection guaranteed by the U.S. authorities.

The EDPB clearly reserved judgment on the final outcome:

> The EDPB will examine how this political agreement translates into concrete legal proposals to address the concerns raised by the Court of Justice of the European Union (CJEU) in order to provide legal certainty to EEA individuals and exporters of data.

It:

> remains committed to playing a constructive part in securing a transatlantic transfer of personal data that benefits EEA individuals and organisations. The EDPB stands ready to provide the European Commission with support to help it build, together with the U.S., a new framework that fully complies with EU data protection law.

However, it would still have to "carefully assess" the "concrete legal proposals", as and when they emerge:

> in the light of EU law, the case-law of the CJEU and the recommendations the EDPB made on that basis. The EDPB will prepare its opinion when it receives from the European Commission all supporting documents.

More specifically, the EDPB will:

> - analyse in detail how [the reforms as ultimately formulated] ensure that the collection of personal data for national security purposes is limited to what is strictly necessary and proportionate;
> - examine to what extent the announced independent redress mechanism respects the EEA individuals' right to an effective remedy and to a fair trial. In particular, the EDPB will look at whether any new authority part of this mechanism has access to relevant information, including personal data, when exercising its mission and can adopt decisions binding on the intelligence services; and
> - consider whether there is a judicial remedy against this authority's decisions or inaction.
>
> (indents added)

4. Issues that will need to be clarified and resolved in any "concrete legal proposals"

Ian Brown and I first addressed separately the likelihood of adequate protection being ensured by US federal or state laws and whether, if this was unlikely, a solution could still be based on a self-certification scheme, and the issue of undue access to data by US agencies, while bringing our conclusions on both these issues together in the final section of our report. We found that there were serious issues with both, and that no positive adequacy issue could be issued until both were addressed.

It is notable that the announcement of the in-principle agreement is silent on the first topic, and limited as concerns the latter – but both will need to be addressed in the "concrete legal proposals".

4.1 General adequacy/self-certification

On this first issue, we concluded as follows:[4]

> Given that ... it will be difficult (if not impossible) to enact any broad US federal privacy law that can meet the substantive requirements of EU law and impose those standards on US corporations, the basic idea of relying on voluntary self-certification by US corporations of compliance with EU level standards, with enforcement if they fail to adhere to their promises, remains the best way forward.
>
> However, any arrangement on that basis would have to be very different from the (rightly invalidated) Safe Harbour and Privacy Shield arrangements – and would require legislative steps by the US (and, we suggest, in one respect by the EU) in relation to substance, enforcement and individuals' rights of action. (And of course the issue of undue access to data by US authorities also needs to be addressed.)

We indicated the kinds of substantive and enforcement changes and changes in relation to general individuals' rights of action that would be required to ensure that any self-certification scheme could provide "essentially equivalent" protection to the EU GDPR.[5]

Here, it will suffice to note that none of these matters are even hinted at in the announcement of the in-principle agreement.

In our opinion, he EDPB will not be able to issue a positive opinion on any "concrete legal proposals" unless those also address the issues of general inadequacy of US privacy law, taking into account the crucial details of any new self-certification scheme – if indeed a new, much enhanced scheme is envisaged. If it is not, there can be no new adequacy decision even if the surveillance regime were to be adequately reformed.

4.2 US Surveillance law

The in-principle announcement instead focussed solely on reform to the US surveillance arrangements. In our study, we noted four (closely interrelated) areas of inadequacy in that respect:

- the fact that US surveillance is not aimed solely at safeguarding the country's national security, but under the applicable rules can be used to serve much broader US interests;
- the lack of safeguards to ensure that the surveillance was limited and targeted ("necessary and proportionate", even in relation to what can properly be regarded as the safeguarding of national security);
- the use of "secret laws" to regulate the surveillance (and/or to change or relax the conditions for and parameters of the surveillance); and
- the absence of an effective redress mechanism in relation to surveillance.

We made clear that, in our opinion, no new positive adequacy decision on the USA could be issued unless all four of these issues were properly addressed.

---

[4] Brown/Korff Study (footnote 1, above), section 4.2.3, *Proposed institutional, substantive and procedural reforms in relation to general adequacy*, p. 106.

[5] *Idem*. For details, see the discussion in that section of the study, under these headings.

4.2.1 "Foreign intelligence" vs. "national security"

In respect of the first point, we note the thrice-repeated reference in the announcement to reform of the legal instruments that regulate US "signal intelligence activities". The aim, it says, is:

> to ensure that signals surveillance activities are necessary and proportionate in the pursuit of defined national security objectives.

However, the aim of US bulk surveillance (the collection of "signals intelligence information") is not limited to "the pursuit of defined national security objectives". Rather, as noted in our study:[6]

> "Foreign intelligence information" (i.e., information that may be collected under FISA) is very broadly defined. In relation to non-US persons, it includes not only information that relates to threats against the USA (§ 1801, para. (e)(1)), but also:
>
> information with respect to a foreign power or foreign territory that relates to, … —
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.
>
> (§ 1801, para. (e)(2). In relation to US persons the information must be "necessary" for these purposes.)

These broad powers have been abused by the USA to spy also on allies and leading allied politicians, and to obtain sensitive commercial and economic information.[7]

This contrasts with the concept of national security in the EU treaties – which was defined by the Court of Justice of the EU in its *LQDN* judgment as follows:[8]

> That responsibility [to safeguard national security] corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities.

The promise in the in-principle announcement, that the legal proposals, when they are released, will "*ensure that [US] signals surveillance activities [will be restricted to what is] necessary and proportionate in the pursuit of defined national security objectives*" cannot be fulfilled if under the relevant US instruments – notably FISA – those activities can continue to be aimed at collecting "*foreign intelligence information*" as currently defined. Either the definition of "*foreign intelligence information*" in FISA must be changed, or the US surveillance activities in relation to the EU must be otherwise expressly and formally limited to measures to ensure US *national security*, with *national security* defined in accordance with the above CJEU interpretation. If neither is done, any reform to US surveillance law will continue to fail to meet EU requirements.

---

6 Brown/Korff Study (footnote 1, above), section 3.2.1, *Overview of FISA s.702, E.O. 12333 and PPD-28*, p. 89.

7 *Idem*.

8 CJEU, judgment in cases Case C 511/18, Case C 512/18 and Case C 520/18, *La Quadrature du Net*, 6 October 202, ECLI:EU:C:2020:791, para. 135, repeated *verbatim* in Case C-140/20, *Commissioner of An Garda Síochána*, 5 April 2022, ECLI:EU:C:2022:258, para. 61.

4.2.2 "Necessary and proportionate"

The Court of Justice of the EU (CJEU) described the US surveillance activities authorised under E.O. 12333 and PPD-28 as:[9]

> '"bulk" collection … of a relatively large volume of signals intelligence information or data under circumstances where the Intelligence Community cannot use an identifier associated with a specific target … to focus the collection'.

It concluded that those instruments:[10]

> [do] not ... delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data.

In its various judgments, the Court has made clear that the question of how to assess whether relevant rules limit the scope of bulk collection in a "sufficiently clear and precise manner", and whether they were "necessary and proportionate", should be answered with reference to the **purpose** of the measure (since the necessity and proportionality of any measure of course always depend on the purpose of the measure). Thus, in relation to **fighting serious crime** or **preventing a serious risk to public security**, the Court held in *Tele2/Watson* that the mandatory retention of traffic and location data must be limited to:[11]

> a public [that is: a section of the general population] whose data is likely to reveal a link, at least an indirect one, with serious criminal offences ...
>
> [The relevant limits] may be set by using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences.

The requirements in relation to measures adopted to **safeguard national security** are less demanding, although there still are important conditions: surveillance measures that seriously interfere with fundamental rights for that purpose (such as, again, mandatory data retention duties) must relate to:[12]

> **a threat to national security [that is] genuine and present, or, at the very least, foreseeable**, which presupposes that **sufficiently concrete circumstances** have arisen to be able to justify a generalised and indiscriminate measure of retention of traffic and location data **for a limited period of time**.

In this regard, threats to national security (as defined by the Court: see the previous sub-section) must be clearly distinguished from other threats:[13]

---

9 CJEU, judgment in Case C-311/18, *Schrems II*, 16 July 2020, ECLI:EU:C:2020:559, para. 183 (quoting a letter from the Office of the Director of National Intelligence to the United States Department of Commerce and to the International Trade Administration from 21 June 2016, set out in Annex VI to the Privacy Shield Decision).

10 *Idem*.

11 CJEU, judgment in Cases C-203/15 and C-698/15, *Tele2/Watson*, 21 december 2016, ECLI:EU:C:2016:970, para. 111.

12 CJEU, *Commissioner of An Garda Síochána* (footnote 8, above), para. 62, emphases added.

13 *Idem*, paras. 62 – 63, with reference to *LQDN*.

> Such a threat [to national security] is ... distinguishable, by its nature, its seriousness, and the specific nature of the circumstances of which it is constituted, from the general and permanent risk of the occurrence of tensions or disturbances, even of a serious nature, that affect public security, or from that of serious criminal offences being committed ...
>
> [C]riminal behaviour, even of a particularly serious nature, cannot be treated in the same way as a threat to national security. As the Advocate General observed in ... his Opinion, to treat those situations in the same way would be likely to create an intermediate category between national security and public security for the purpose of applying to the latter the requirements inherent in the former.

In other words, under EU law, measures that may be justified to safeguard national security (i.e., that are "necessary and proportionate" for that purpose) – as strictly and restrictively defined – may not be justified (may not be "necessary and proportionate") in relation to more general aims such as protecting public security, fighting serious crime or ensuring public order. And even the former (measures to safeguard national security) must be strictly limited to situations in which there are concrete indications that there is a genuine and immediate or clearly foreseeable threat to "the essential functions of the State and the fundamental interests of society".

It should be clear from the above that <u>it will not suffice</u> for the promise in the in-principle announcement, that the legal proposals, when they are released, will "*ensure that [US] signals surveillance activities [will be restricted to what is] necessary and proportionate in the pursuit of defined national security objectives*" to be fulfilled, that those activities will be limited to national security objectives as defined by the CJEU (although that is a precondition: see the previous sub-section).

Rather, <u>in addition</u>, any new rules regulating to those activities will have to limit those activities to situations in which there is "*a genuine and immediate or clearly foreseeable threat to the essential functions of the USA and the fundamental interests of American society*".

The current rules (FISA, E.O. 12333 and PPD-28), by contrast, allow collection by the US intelligence agencies of any "*information with respect to a foreign power or foreign territory that <u>relates to</u> the national defense or the security of the United States or the conduct of the foreign affairs of the United States*"; the information does not even need to be "necessary" for those in any case sweeping purposes.

Unless the US rules on surveillance including its signals surveillance are fundamentally reformed to reflect the EU standards of necessity and proportionality – and applied only to national security as defined by the CJEU – US surveillance law will continue to fail to meet EU requirements.

4.2.3 Secret laws

We noted in our report that US surveillance activities can, to a considerable extent, be regulated by unpublished – i.e., secret – rules or interpretations. It will suffice to reproduce the relevant short section here:[14]

While the publication of E.O. 12333 and PPD-28 provides a greater level of transparency than in many other countries,[15] it is still the case that "the President may 'modify' or 'waive' them simply by departing from their terms, without providing any notice to the public."[16]

Even with statutory provisions, the US Department of Justice's Office of Legal Counsel (OLC) regularly issues classified legal interpretations on national security matters which are binding on the executive branch. If a court later disagrees, the Justice Department will still not "investigate or prosecute somebody for acting in reliance" on such an opinion.[17] Such opinions were used during the George W. Bush administration to justify US torture and warrantless surveillance, with a later Bush-appointed attorney-general (Jack Goldsmith) observing OLC lawyers dealt with the Foreign Intelligence Surveillance Act "the way they dealt with other laws they didn't like: they blew through them in secret based on flimsy legal opinions that they guarded closely so no one could question the legal basis for the operations."[18]

Congressional committees, particularly the permanent intelligence committees, frequently issue reports with classified annexes. Some of these are important for the interpretation of statutes, and in some cases their provisions are incorporated by reference into legislation.[19] And the Foreign Intelligence Surveillance Court's decisions, such as authorising surveillance programmes under FISA s.702, can contain significant legal interpretations. One example was the Court's interpretation of s.215 of the Patriot Act, on whether business records sought by the government were "relevant" to a terrorism investigation, to cover almost every American's phone records.[20]

While important FISC opinions have been declassified and published by the Director of National Intelligence, which is now required by the USA Freedom Act of 2015, one 2016 assessment "ascertained that most of the significant pre-Snowden FISA case law remains undisclosed, including 25-30 still-classified opinions or orders issued between mid-2003 and mid-2013 that were deemed significant by the Attorney General."[21]

---

14 Brown/Korff Study (footnote 1, above), section 3.2.2, *"Secret law"*, pp. 91 – 92.

15 Ian Brown, Morton H. Halperin, Ben Hayes, Ben Scott and Mathias Vermeulen, Towards Multilateral Standards for Surveillance Reform, In Russell A. Miller (ed., 2017) *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair,* Cambridge University Press, pp.461–491.

16 Elizabeth Goitein, *The New Era of Secret Law*, Brennan Center for Justice at New York University School of Law, 2016, p.5, at:
https://www.brennancenter.org/sites/default/files/2019-08/Report_The_New_Era_of_Secret_Law_0.pdf

17 *Idem*, p.37.

18 *Idem*, p.38.

19 *Idem*, pp.29—31.

20 *Idem*, p.58.

21 *Idem*, p.6.

We concluded that:[22]

> The US laws described [in our study] do not meet the European standards that the legal rules on surveillance must be accessible (i.e., published), legally binding, clear, precise and "foreseeable" in their application.

The promise in the in-principle announcement, that the legal proposals, when they are released, will "*ensure that [US] signals surveillance activities [will be restricted to what is] necessary and proportionate in the pursuit of defined national security objectives*" cannot be fulfilled, for as long as the President can still "modify" or "waive" the applicable rules, or secret but effectively binding interpretations determine how they are applied. Rules that interfere with fundamental rights – as all rules on state surveillance do by their very nature – only meet EU (and broader European) standards if they are clear and published and foreseeable in their application. Secret US rules and secret US interpretations of the rules can never provide "essentially equivalent" protection to individuals as is accorded by EU legal rules. Even the very possibilities of secret changes to the rules or their interpretation are incompatible with European concepts of the rule of law.

4.2.4 Effective redress in relation to surveillance

As we noted in our study (with reference to a study commissioned by the US Congress):

> Like E.O. 12333, PPD-28 does not purport to provide judicially enforceable rights for private persons who may have been subject to surveillance in violation of the directive's provisions… [Apart from in some special circumstances], there is generally no opportunity for targets of surveillance to know whether their communications or information have been acquired by the government under Section 702, and as a result, fewer opportunities may exist to seek judicial review of that acquisition.

The announcement of the new arrangements expressly promises to address this:

> [Under the Trans-Atlantic Data Privacy Framework, the United States will] establish a two-level independent redress mechanism with binding authority to direct remedial measures, and enhance rigorous and layered oversight of signals intelligence activities to ensure compliance with limitations on surveillance activities.

The Article 29 Working Party has pointed out, with reference to the *Schrems I* judgment, that, in relation to the issue of access to data by third country intelligence agencies:[23]

> [a]lthough the means to which the third country has recourse for the purpose of ensuring an adequate level of protection may differ from those employed within the European Union, a system consistent with the European one must be [in place].

This required that the redress system in place should be "*characterized by the existence of the following elements*":[24]

---

22 *Idem*, section 3.2.3, *Assessment by EU standards*, p. 93.

23 WP29 *Adequacy Referential*, section C.

24 *Idem* (paraphrased)

- there must be one or more "completely independent" and impartial supervisory authorities with effective supervisory and enforcement powers;
- the system should ensure "a good level of compliance" in practice, which can be ensured through sanctions, verifications and audits;
- the system should ensure accountability, by "oblig[ing] data controllers and/or those processing personal data on their behalf to comply with it and to be able to demonstrate such compliance in particular to the competent supervisory authority", e.g., through data protection impact assessments, the keeping of records or log files of data processing activities, the designation of data protection officers, or data protection by design and by default; and
- the system must provide "support and help to individual data subjects in the exercise of their rights and appropriate redress mechanisms".

The promises in the in-principle announcement of "*a two-level independent redress mechanism with binding authority to direct remedial measures*" and of "*enhance[d] rigorous and layered oversight of signals intelligence activities to ensure compliance with limitations on surveillance activities*" will only provide the required levels of protection if they fully include the above-listed elements of an appropriate redress mechanism.

5. Overall conclusion

The promise in the in-principle announcement, that the legal proposals, when they are released, will "*ensure that [US] signals surveillance activities [will be restricted to what is] necessary and proportionate in the pursuit of defined national security objectives*" cannot be fulfilled unless:

- **either the definition of "foreign intelligence information" in FISA is changed, or the US surveillance activities in relation to the EU are otherwise expressly and formally limited to measures to ensure US national security, with national security defined in accordance with the strict CJEU interpretation of that concept (which is fundamentally different from the current purpose of surveillance as authorised under FISA);**
- **new rules regulating to US surveillance activities will limit those activities to situations in which there is "*a genuine and immediate or clearly foreseeable threat to the essential functions of the USA and the fundamental interests of American society*";**
- **none of those rules, and no interpretations of those rules, are adopted or issued in secret (or can subsequently be modified or re-interpreted in secret); and**
- **the new redress and oversight systems fully include all the elements set out for such systems by the Article 29 Working Party.**

There is little in the announcement of the "political"/"in principle" agreement that suggests that these high standards will be met. If, when the promised "concrete legal proposals" are revealed, they fail to meet those standards, the EDPB should emphatically refuse to issue a positive opinion on them.

- 0 – O – o –