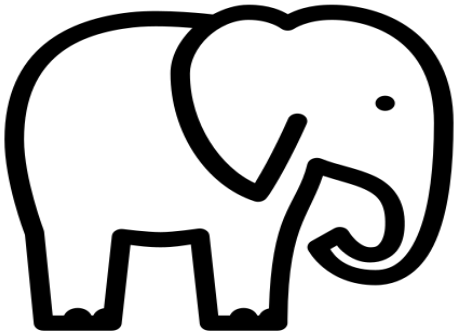
The inadequacy of the
EU Commission Draft GDPR Adequacy Decision on the UK

by

Douwe Korff
Emeritus Professor of International Law, London Metropolitan University
Visiting Fellow, Yale University (Information Society Project)
Associate, Oxford Martin School, University of Oxford

A tale involving an elephant and three monkeys



3 March 2021

Douwe Korff
Emeritus Professor of International Law, London Metropolitan University
Visiting Fellow, Yale University (Information Society Project)
Associate, Oxford Martin School, University of Oxford

About this paper:

This paper provides critical comments on the European Commission's Draft Implementing Decision pursuant Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, released on 19 February 2021, available at: https://service.betterregulation.com/document/488712

It follows on from a series of submissions on the issue by the author and Prof. Ian Brown to EU bodies and officials involved in the taking of this decision and some further comments issued since, that can be found here:

Korff-Brown Submission to EU re UK adequacy, Part One *re* general inadequacy, 9 October 2020, available at:
https://www.ianbrown.tech/2020/10/09/the-uks-inadequate-data-protection-framework/

Korff-Brown Submission to EU re UK adequacy, Part Two *re* UK surveillance, 30 November 2020, available at:
https://www.ianbrown.tech/wp-content/uploads/2020/11/Korff-Brown-Submission-to-EU-re-UK-adequacy-Part-Two-DK-IB201130.pdf

Korff-Brown Submission to EU *re* UK adequacy, Executive Summary (with a discussion of the implications for the UK, other third countries and the EU, 30 November 2020, available at:
https://www.ianbrown.tech/wp-content/uploads/2020/11/Korff-Brown-Submission-to-EU-re-UK-adequacy-ExecSumm-DK-IB201130.pdf

Douwe Korff, *"The United Kingdom is not a third country under EU law"*, 2 January 2021, available at:
https://www.ianbrown.tech/2021/01/02/the-united-kingdom-is-not-a-third-country-under-eu-law/

Douwe Korff, *UK adequacy, international transfers, and human rights compliance*, 2 February 2021, available at:
https://www.ianbrown.tech/2021/02/02/uk-adequacy-international-transfers-and-human-rights-compliance/

About the author:

Douwe Korff is a Dutch comparative and international lawyer specialising in human rights and data protection. He is emeritus professor of international law at London Metropolitan University and visiting professor at the universities of Zagreb and Rijeka in Croatia; an Associate of the Oxford Martin School of the University of Oxford, a Visiting Fellow at Yale University (Information Society Project), and a Fellow at the Centre for Internet and Human Rights of the European University of Viadrina, Berlin.

Acknowledgment: I am grateful to Prof. Ian Brown for his helpful comments on an earlier draft of this paper. All errors of course remain entirely mine.

Douwe Korff
Emeritus Professor of International Law, London Metropolitan University
Visiting Fellow, Yale University (Information Society Project)
Associate, Oxford Martin School, University of Oxford

The inadequacy of the EU Commission Draft GDPR Adequacy Decision on the UK

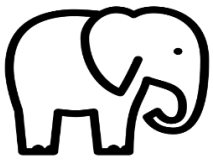
CONTENTS:

- o – O – o -

Douwe Korff
Emeritus Professor of International Law, London Metropolitan University
Visiting Fellow, Yale University (Information Society Project)
Associate, Oxford Martin School, University of Oxford

AT A GLANCE:

- The Draft Decision generally looks at the law on paper (as described, at times misleadingly, by the UK itself) without paying any real attention to the application of the law in practice and without assessing law or practice against the EU legal standards.
- The UK rules on data sharing, the immigration exemption and the research exemption are clearly not in accordance with the EU standards.
- Adoption of the decision would lead to **serious risks** that the UK will become a data protection-evasion haven for personal data from the EU/EEA to countries that are not held to provide adequate protection by the EU; that the UK will allow for undue direct access to data (including data on EU persons) by US authorities under the UK-US Agreement; and that it will allow UK companies to meekly comply with judgments and orders from non-EU Member States, also in respect of EU data, contrary to Article 48 GDPR.
- The UK ICO continues to fail to properly enforce the law in the vast majority of cases – even when it itself concludes that the law has been broken.
- **The elephant in the room: The Draft Decision completely fails to assess (or even note) the UK's intelligence agencies' actual surveillance practices.**



The Commission simply does not want to see or hear about or talk about these practices. It ignores that:

- ✓ there is no effective substantive oversight by the ICO or the courts over the use of the national security exemption in UK data protection law;
- ✓ the limitations on the use of UK "bulk powers" are not set out in the law itself, as required by the CJEU (but rather, are left to executive discretion subject to very marginal, "respectful" judicial review);
- ✓ the description of "secondary data" (metadata) in the Draft Decision is **seriously misleading** and fails to note that such data can be highly revealing and intrusive and are subject to sophisticated automated analyses. Yet under UK data protection law metadata are not meaningfully protected against undue access, bulk collection and AI-based analysis by the UK intelligence agencies.
- ✓ the "5EYES" agencies, and more in particular GCHQ and the NSA, in practice share effectively all intelligence data.

- Given the lack of action by the Commission in relation to other adequacy decisions, not too much should be expected of the "ongoing monitoring" by the Commission of the situation in the UK after the UK decision comes into force (if it ever does).

Douwe Korff
Emeritus Professor of International Law, London Metropolitan University
Visiting Fellow, Yale University (Information Society Project)
Associate, Oxford Martin School, University of Oxford

The inadequacy of the EU Commission Draft GDPR Adequacy Decision on the UK

=== EXECUTIVE SUMMARY ===

General comments:

The Draft UK Adequacy Decision:

- relies on uncritically copied-and-pasted descriptions of UK law and practice by the UK Government;
- briefly – much too briefly – mentions the standards set by the CJEU and the EDPB that should be applied to UK law and practice – but then does not actually apply those standards;

and fails to note that:

- even EU law, case-law and general principles that are supposed to be "retained" in UK law can already be discarded by ministerial order or judicial re-interpretation (by the highest UK courts);
- in any case the UK is no longer bound by post-1 January 2021 CJEU judgments in relation to data protection (while several important cases are pending), i.e., that alignment with EU law in this regard is not "dynamic";
- the UK Government has made very clear that it wants to diverge from EU data protection law and also include flows of (personal) data in trade agreements including the much hoped-for FTA with the USA (contrary to the EU horizontal policy that personal data should not be included in such agreements); and
- in some contexts, such as immigration and national security, lip service is paid in the text of the law to necessity and proportionality but with limited effect in practice.

The Draft Decision generally looks at the law on paper (as described, at times misleadingly, by the UK itself) without paying real attention to the application of the law in practice and without assessing law or practice against the EU legal standards.

Specific issues:

I. General adequacy issues:

1. **Data sharing:** The UK rules on the sharing of personal data (and in particular lightly pseudonymised data) are clearly not "essentially equivalent" to the EU rules (even if one has to look beyond the simple text of the UK GDPR to note this).

2. Exemptions:

2.1 **Immigration exemption:** In the – for EU citizens and other non-UK nationals in the UK, crucial – immigration context, the UK data protection rules are both on paper and in practice clearly not "essentially equivalent" to the EU ones (as set out in the GDPR).

2.2 **Research exemption:** Contrary to what is allowed under the EU GDPR, the exemption in the UK GDPR relating to processing for research purposes also allows departure from the rules on international data transfers.

Douwe Korff
Emeritus Professor of International Law, London Metropolitan University
Visiting Fellow, Yale University (Information Society Project)
Associate, Oxford Martin School, University of Oxford

3. Data transfer issues:

3.1 **Semantics:** The UK and the Commission make an indefensible distinction between "transfers" and "transits" and "merely routing" of data. This playing with words is an attempt to exclude "simple routing of data" through third countries and "direct collecting of personal data" by third country entities (private and public) directly from data subjects in the EU/EEA from the rules in the GDPR on international transfers – and onward transfers. If the UK and EU Commission views were to be allowed to pass, that would drive a coach and horses through *Schrems II*, *PI*, *LQDN* and other judgments, and through the EDPB's European Essential Guarantees for surveillance.

3.2 **Onward transfers on the basis of UK-issued adequacy decisions:** The UK has given its own authorities the power to declare that other third countries provide "adequate" protection in terms of the UK GDPR – and the UK has already shown it is willing to declare territories as providing such adequacy even when the EU has not done so.

> Unless there are watertight assurances from the UK Government that it will not declare any non-EU/EEA country to provide adequate protection under the UK GDPR unless that country is also held by the EU to provide adequate protection under the EU GDPR, and that it will suspend or withdraw any UK-issued adequacy decision on any country in respect of which the EU invalidates, suspends or withdraws its adequacy decision, the UK will become a data protection-evasion haven for personal data from the EU/EEA to countries that are not held to provide adequate protection by the EU (or in respect of which a previous decision was invalidated, suspended or revoked), including the other "5EYES" countries (USA, Canada, New Zealand and Australia).
> **The Draft Decision provides no assurances to that effect.**

3.3 **Onward transfers on the basis of the UK-USA Agreement:** In the Draft Decision the Commission accepts transfers (including onward transfers) from the UK to the USA under the recently signed UK-USA Agreement because (in the Commission's view) it provides for "equivalent protections to the specific safeguards provided by the so-called 'EU-US Umbrella Agreement'" – but not only are there still serious doubts about the Umbrella Agreement, the UK also only promises that it will apply the Umbrella Agreement safeguards "*mutatis mutandis*" with "*adaptations to reflect the nature of the transfers at issue*". The Commission says it will monitor how this will work out – but that is not a sufficient safeguard: see below, at III.

3.4 **Compliance with foreign judgments and orders:** The relationship between Article 48 GDPR and the remainder of Chapter V, in particular Articles 46 and 49, is unclear. But it was clearly the intention of the EU legislator (in particular the EP) that Member States should bar companies under their jurisdiction from meekly complying with judgments and orders from non-EU Member States; that the same should apply in relation to onward transfers from third countries; and that that should be reflected in all adequacy decisions. But the information provided by the UK makes clear that the UK effectively wants to ignore and bypass that constraint – and the Commission is willing to collude in that.

3.5 **Oversight and enforcement:** It is difficult to see how the Commission – had it looked seriously at the statistics – can have concluded that the ICO "identifies and punishes"

transgressors "in practice" and "imposes [appropriate] sanctions" on controllers and processors who break the law. In fact, on the contrary, the ICO continues to fail to properly enforce the law in the vast majority of cases – even when it itself concludes that the law has been broken.

II. Issues relating to UK national security and bulk surveillance powers:

1. **The elephant in the room:** The Draft Decision completely fails to assess (or even note) the UK's intelligence agencies' actual surveillance practices. It does not mention the Snowden revelations, or the US-UK "TEMPORA" programme, or the joint UK-US bulk interception station in Bude, Cornwall, or what it is used for, or the European Parliament's report on US surveillance (which is also extremely relevant to the UK), or Caspar Bowden's report to the EP, or the UK NGO Open Rights Group's excellent and detailed reports into the UK surveillance practices and laws, or Eric King's witness statement on behalf of Privacy International in the case before the UK Investigatory Powers Tribunal (or our own summaries of these matters). The Commission appears to believe that all this need not be looked at because, while the Draft Decision actually confirms that the bulk data collected by the UK intelligence agencies also includes data on EU persons, it only forms a small part of the massive global UK-USA (and other "5EYES") surveillance programmes.

   Hopefully, the EDPB and the EP will seek further details on this issue – and will not accept that UK surveillance of and bulk data collection on EU persons can be ignored because it "does not happen normally" or all that often (comparably speaking).

2. **The national security exemption:** Neither the relevant legal provisions nor the ICO-UK Intelligence Community MoU "ensure" that the exemption from data protection rights in the UK GDPR is only used when objectively necessary and proportionate to protect national security. They place an obligation on the part of the authorities issuing a "conclusive" certificate to consider the necessity and proportionality of the certificate – but do not involve effective substantive oversight by the ICO or the courts to ensure this is properly done. This raises doubts about the compatibility of the law with fundamental (EU CFR) requirements.

3. **Limitations on the use of the UK "bulk powers":** The UK law allowing for the use of bulk powers (the IPA) does not in itself, on its face, specify the nature of offences which may give rise to the issuing of a bulk powers warrant (rather, they can be used in relation to any "interests of national security", including the "economic wellbeing of the UK" and "preventing and combating serious crime" when related to national security), and that law also does not, in itself, on its face, define the categories of people on whom data can be collected under the bulk power warrants. Those matters may well, to some extent, be addressed in the processes concerned – but that is not the same as specifying them in the law itself. That is clearly not in accordance with the case-law of the CJEU and the ECtHR, or with the EDPB's European Essential Guarantees.

4. **The nature and use of the data obtained in bulk:** The description of "secondary data" (metadata) in the Draft Decision is seriously misleading. It fails to note that such data can be highly revealing and intrusive and are subject to sophisticated automated analyses. Yet under UK data protection law:

- metadata are not meaningfully protected against undue access and bulk collection by the UK intelligence agencies;
- the situation in relation to oversight over complex selectors and search criteria is still unclear; while
- oversight over the much more sophisticated data mining analyses appears to not have been addressed at all.

The situation relating to the processing of metadata ("secondary data") by the UK intelligence agencies therefore clearly does not meet the EU standards as set out, in particular, in the CJEU LQDN judgment, referenced in this regard in the EEGs.

5. **Transfer of data obtained in bulk to other third countries:** The extensive – indeed, it would appear, comprehensive – data sharing arrangement between the "5EYES" agencies, and more in particular between GCHQ and the NSA, means that data on individuals in the EU, and in particular their communications data, collected in bulk by GCHQ, will (continue to) be made available also to the NSA – and indeed analysed in the manner described earlier jointly by GCHQ and NSA staff. In terms of the GDPR, this sharing will, at least from 1 January 2021, involve the "onward transfer" of the data on individuals in the EU from the UK to the USA.

   While the UK was an EU Member State, perhaps not much could be done about this under EU law. However, now that the UK is no longer an EU Member State this can, and we submit must, be addressed urgently, in general and in the context of the matter of a UK adequacy decision.

   But once again, the Draft Decision effectively ignores this crucial issue.

III. Monitoring of the adequacy decision:

In line with all other adequacy decisions, the Draft Decision says that the Commission will "monitor the developments" in relation to data protection in the UK after the coming into force of the decision, "on an ongoing basis"

However, in practice, the Commission has **never** repealed, suspended or amended any adequacy decision even when it would be clear from even a cursory examination of a country's law and practices that (whatever the original situation when assessed under the 1995 Directive) the country does not provide for adequate protection in terms of the GDPR, as clarified by the CJEU in *Schrems I* ("essentially equivalent").

In the circumstances, not too much should be expected of the "ongoing monitoring" by the Commission of the situation in the UK after the UK decision comes into force (if it ever does).

- o – O – o -

Douwe Korff (Prof.
Cambridge, UK, 3 March 2021

Douwe Korff
Emeritus Professor of International Law, London Metropolitan University
Visiting Fellow, Yale University (Information Society Project)
Associate, Oxford Martin School, University of Oxford

The inadequacy of the EU Commission Draft GDPR Adequacy Decision on the UK[1]

General comments:

1. The descriptions of UK law including of the UK DPA2018, the UK GDPR and the IPA appear to be taken directly from descriptions provided by the UK itself which are essentially uncritically copied-and-pasted into the EU Commission decision after some introductory sub-sections (as to which, see below, at 2).

This means that a number of vague or even somewhat (or more than somewhat) misleading descriptions of the law or attempts to introduce distinctions unknown to EU law are left effectively unchallenged and even unanalysed. Examples are given in section II, *passim*.

2. The Commission writes in its Draft Decision that "*[t]he standard against which the 'essential equivalence' is assessed is that set by European Union legislation, notably Regulation (EU) 2016/679, as well as the case law of the Court of Justice of the European Union*", and that "*[t]he European Data Protection Board's adequacy referential is also of significance in this regard*" (recital 3). However, in practice almost no effort is made to actually relate the Commission's conclusions about the adequacy of various UK legal rules and practices explicitly to any of these standards.

The case-law of the CJEU is barely mentioned other than in these introductory sub-sections – and never to actually assess the relevant UK legal rules in the light of specific case-law requirements. The Adequacy Referential is completely ignored and no longer mentioned at all after recital 3.

3. In the general introductory section of the Draft Decision, the Commission explains that the EU GDPR continues to be applicable in the UK as "**retained EU law**" and is for the time being amended only "to fit the domestic context"; and that the relevant case law of the European Court of Justice and general principles of Union law as they had effect immediately before the end of the transition period also continue to apply for the time being in what are called "**retained EU case law**" and "**retained general principles of EU law**" respectively (see recitals 12 – 16 of the Draft Decision).

However, this is not as reassuring as it is made to appear. First of all, the Draft Decision does not make clear that:[2]

---

[1] The various paragraphs in the report on UK adequacy are referred to in the Commission Draft Adequacy Decision as recitals – because technically they are in the part of the document that leads up to the actual draft decision. For consistency sake, I have done the same in this note.

[2] UK Ministry Of Justice, Retained EU Case Law – Consultation on the departure from retained EU case law by UK courts and tribunals, 2 July 2020, p. 6, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896830/retained-eu-case-law-consultation.pdf
This refers to the European Union (Withdrawal) Act 2018 (Relevant Court) (Retained EU Case Law) Regulations 2020 (SI 2020 No. 1525), made on 9 December 2020, available at: https://www.legislation.gov.uk/uksi/2020/1525/introduction/made

> **[T]he UK Supreme Court or the High Court of Justiciary**, as the final criminal court of appeal in Scotland in circumstances where there is no route of appeal to the UK Supreme Court, **have jurisdiction to depart from retained EU case law** [on the basis of the English or Scottish legal] rules they respectively exercise in departing from their own previous case law.
>
> (emphasis added)

This means that the highest UK courts can actually already, now, depart from pre-2021 CJEU judgments including *Schrems II*, *PI* and *LQDN* on English or Scottish legal (rather than EU law) grounds (although, perhaps, setting aside of retained EU case-law in the immediate future may be unlikely).

Perhaps more importantly, therefore, is the fact that UK Government statements and the Draft Decision make clear that **the alignment of UK law with EU law, case-law and general principles is <u>not dynamic</u>: it only applies to "*the relevant case law of the European Court of Justice and general principles of Union law as they have effect immediately before the end of the transition period*"** (see recital 12 of the Draft Decision).

Any judgments adopted by the CJEU after 1 January 2021 – e.g., further judgments on surveillance by third countries, mandatory data retention, or immigration or research issues – will therefore clearly <u>not</u> be applicable in the UK if the adequacy decision is adopted (and it would seem are already not applicable).[3] There are several important pending cases in these areas. The same applies to any suspension or revocation of EU adequacy decisions adopted before 2018 – which are currently all under review (see section II, at 3.2).

Overall, the UK alignment with EU data protection law including the GDPR is therefore not as full or unconditional as the Draft Decision suggests – not even now.

4. Moreover, given that it was one of the main aims of the Brexiteers to diverge from EU law (including EU data protection law) and more specifically to "shake off the shackles of the EU Court of Justice", it is extremely unlikely that UK data protection law will remain more or less aligned with EU data protection law, in particular the GDPR, even in respect of the actual terms of the law, let alone its interpretation (see General Comment 3, above) – and the Withdrawal Act allows the UK Secretary of State to amend the law at the stroke of a pen, in all material respects, subject to minimal parliamentary oversight. In some respect, UK data protection is already not aligned with EU law (as shown in Part II).

The UK Government also has clearly expressed its intention to divert from EU data protection law including from the GDPR, not least to enable a "data driven economy" that can outcompete the EU in that respect:[4]

---

[3] See the rather odd article in the TCA, Article FINPROV.10A, that stipulates that for the next few month the UK must still be treated as if it were a Member State (in spite of the fact that it is not), but that does not seem to ensure that the UK will be bound by CJEU judgments issued during the "specified period" for which it applies.

[4] New national data strategy 'threatens' UK data adequacy resolution, New Statesman, 15 September 2020, available at:
https://tech.newstatesman.com/policy/new-national-data-strategy-threatens-uk-data-adequacy-resolution-say-experts
Cf. also, e.g., *Firms get public data in Dominic Cummings tech drive*, Times, 14 September 2020:

> In 2018, Dominic Cummings, the Downing Street adviser who [was] driving much of the government's work around technology, **described GDPR as "horrific" legislation. "*One of the many advantages of Brexit is we will soon be able to bin such idiotic laws,*"** he wrote. "*We will be able to navigate between America's poor protection of privacy and the EU's hostility to technology and entrepreneurs.*"
>
> (emphasis added)

This approach of deliberate divergence from the GDPR informed and continues to inform the UK's new "national data strategy" (also after Cummings' departure from Downing Street).[5]

This makes the close monitoring of future developments crucial (irrespective of whether the adequacy decision goes ahead). However, the past inactivity of the Commission in relation to other adequacy decisions is not a good omen in that regard. This is further discussed in the body of this paper, at III.

5. The Draft Decision notes often that UK law requires relevant authorities to comply with basic principles, especially necessity and proportionality, and that the UK courts can review this. It fails to note that in some contexts, in particular immigration and national security, this is sometimes the UK legislator and courts paying lip service to the principles but not really upholding them in practice.

For example:

> The IPA 2016 replaces the legislation concerning the acquisition of bulk communications data which was the subject of the CJEU judgment in the *Privacy International* case. The legislation at issue in that case was repealed and the new regime provides for specific conditions and safeguards under which such measure can be authorised.
>
> In particular, differently from the previous regime under which the Secretary of State had full discretion in authorising the measure, the IPA 2016 requires the Secretary of State to issue a warrant only if the measure is necessary and proportionate. …
>
> (Recitals 227 – 228, footnote omitted)

What the Commission does not note is that this is a rather limited exercise: if the Secretary of State notes in a decision that he is persuaded that what he authorises is necessary and proportionate, the review of that by oversight bodies and courts is marginal at most. Specifically, the courts and the Judicial Commissioners that overview the issuing of "bulk

https://www.thetimes.co.uk/article/firms-get-public-data-in-dominic-cummings-tech-drive-s3s8j33fw

[5] "*Post-Brexit, [the UK] hopes to attract business by differentiating itself from the EU regulatory regime. Oliver Dowden, the culture secretary, is looking to scale back parts of the EU's data protection regime without jeopardising a data-sharing deal.*" Financial Times, 24 February 2021, available at: https://www.ft.com/content/bd8accda-fb12-4664-a8c9-182e80e8000d ($)
Or in the culture secretary's own words: "*We fully intend to main [the UK's] world-class [data protection] standards. But to do so, we do not need to copy and paste the EU's rule book, the General Data Protection Regulation, word for word. Countries as diverse as Israel and Uruguay have successfully secured adequacy with Brussels despite having their own data regimes. Not all of those were identical to GDPR, but equal doesn't have to mean the same. The EU doesn't hold the monopoly on data protection.*" Financial Times, 27 February 2021, available at:
https://www.ft.com/content/ac1cbaef-d8bf-49b4-b11d-1fcc96dde0e1 ($)
In fact, it would appear unlikely that Israel, at least, will continue to be held to provide adequate data protection after the current review: its privacy law is manifestly not adequate in GDPR terms. I make some comments about that in Part III, concerning the monitoring of adequacy decisions by the Commission.

powers" orders (discussed at II.3, below) apply judicial review standards – which are very limited:[6]

> There are three main grounds of judicial review: illegality, procedural unfairness, and irrationality.
>
> A decision can be overturned on the ground of illegality if the decision-maker did not have the legal power to make that decision, for instance because Parliament gave them less discretion than they thought.
>
> A decision can be overturned on the ground of procedural unfairness if the process leading up to the decision was improper. This might, for instance, be because a decision-maker who is supposed to be impartial was biased. Or it might be because a decision-maker who is supposed to give someone the chance to make representations before deciding on their case failed to do so.
>
> A decision can be overturned on the ground of irrationality if it is so unreasonable that no reasonable person, acting reasonably, could have made it. This is a very high bar to get over, and it is rare for the courts to grant judicial review on this basis.
>
> In addition, a decision can be overturned if a public authority has acted in a way which is incompatible with human rights that are given effect by the Human Rights Act 1998. There is one exception to this, though: if the public authority is merely doing what parliament told it to do, then it is not acting unlawfully even if it does act incompatibly with one of those rights.
>
> A judge cannot quash or declare unlawful a government decision merely on the basis that the judge would have made a different decision, or that the decision was wrong.

In fact, the Government believes that this still gives too much power to the judges and wants to limit judicial review further to ensure that it "is not abused to conduct politics by another means or to create needless delays."[7]

In national security cases, the review is even more marginal and deferential: see section II.2, below, with reference to the recent *Begum* judgment.

The Draft Decision generally looks at the law on paper (as described, at times misleadingly, by the UK itself) without paying any real attention to the application of the law in practice. On one of the rare occasions when there is actual reference to practice, with statistics (in relation to enforcement actions by the UK ICO), the details are only provided in a footnote, without the Commission noting that if anything these point to miserable levels of real enforcement (see at I.4, below). In many contexts in which statistics or other details of practice would have been important, they are lacking.

The application of the **immigration exemption**, noted below at 2, is another good (i.e., bad) example.

- o – o – o -

[6] Institute for Government, *Judicial review*, available at: https://www.instituteforgovernment.org.uk/explainers/judicial-review

[7] *Idem*, quoting the Conservative Party manifesto. This intention has been confirmed by leading members of the government and Conservative politicians.

Specific issues:

I. General adequacy issues:

1. Sharing of personal data (recital 22):

The Draft Decision says that

> The definitions of **personal data**, processing, controller, processor, as well as the definition of pseudonymisation, laid down in Regulation (EU) 2016/679 have been retained without material modifications in [Article 3 of] the UK GDPR.

As such, this is correct. However, the Draft Decision nowhere explores the issue of the more limited definition of "*information [that] identifies a particular person*" in the UK 2017 Digital Economy Act. As pointed out in Part One of the Korff/Brown Submission on UK Adequacy:[8]

> This suggests that **while data on unidentifiable but singled-out individuals must, under the (EU) GDPR, be treated as personal (identifiable) data, and can therefore only be shared subject to the various conditions for processing … under the UK DEA – and the UK GDPR – data can be much more widely shared and used.**
>
> **This will also apply to personal data transferred to the UK after the post-Brexit transition period (irrespective of whether they are transferred in identifiable or pseudonymised form).**
>
> (emphasis added, footnotes omitted)

In other words: the Commission has failed to note that when it comes to the sharing of personal data (and in particular lightly pseudonymised data), the UK rules are clearly not "essentially equivalent" to the EU rules (even if one has to look beyond the simple text of the UK GDPR to note this).

This issue is related to the research exemption (discussed below, at 2.2) and to the data transfer regime (discussed below, at 3).

2. Exemptions

2.1 The immigration exemption (recitals 62 – 66):

While acknowledging that the UK immigration restriction (as it calls it) is "*formulated rather broadly*", the Commission still find it acceptable in terms of the GDPR because "*it must be applied on a case-by-case basis, only to the extent necessary to achieve a legitimate aim and in a proportionate manner*" (recital 65). Typically, the Commission then does not go on to assess whether in fact, in practice, the exemption/restriction *is* applied in such a manner.

Yet as the UK *Open Rights Group* (ORG) has shown, in fact the exemption, rather than being invoked only in exceptional, rare cases (as the UK Government assured Parliament it would when it introduced the rule), is invoked by the UK authorities in the vast majority of cases in which non-UK nationals (including EU citizens) try to exercise their data protection right of access to their data: the Home Office denies such access in approximately three quarters of all access requests – and thereby also fundamentally undermines the rights of the individuals

[8] Korff-Brown Submission to EU re UK adequacy, Part One *re* general inadequacy, 9 October 2020, section 3.2.1, available at: https://www.ianbrown.tech/2020/10/09/the-uks-inadequate-data-protection-framework/

concerned to effectively challenge any Home Office decisions based on the inaccessible and therefore unchallengeable data.[9]

The test under the "*rather broadly formulated*" immigration exemption – whether granting an individual access to (all or part) of their file might "prejudice" effective immigration control – is therefore clearly much less demanding than the GDPR Article 23 test of whether denial of access is "necessary" and "proportionate".

The UK authorities provided the following example as proof of why the "broadly phrased" exemption is necessary:

> [i]f a suspected terrorist under active investigation by MI5 made an access request to the Home Office (for instance, because he is engaged in a dispute with the Home Office over immigration matters), it would be necessary to protect from disclosure to the data subject any data that MI5 may have shared with the Home Office relating to ongoing investigations that could prejudice sensitive sources, methods or techniques and/or lead to an increase in the threat posed by the individual.
>
> (footnote 67)

This is a complete red herring: there would in this case be ample other legal grounds for denying the suspected terrorist access to the data that could "*prejudice sensitive sources, methods or techniques and/or lead to an increase in the threat posed by the individual*". Interestingly, in the domestic debates the relevant minister had used the less emotive – but still equally misleading – example of a suspected overstayer receiving disclosure via a subject access request that the Government are preparing an administrative removal and would be able to evade enforcement action. Clearly, the UK Government felt that the Commission would be more impressed by a terrorism related (though still false) example. And it seems to have worked.

In other words, in this – for EU citizens and other non-UK nationals in the UK, crucial – context, the UK data protection rules are therefore *both on paper and in practice* clearly not "essentially equivalent" to the EU ones (as set out in the GDPR). But the Commission fails to acknowledge this – or even to properly examine the facts (or the example).

2.2 The research exemption (recital 73):

The Draft Decision says (in what would again appear to be quote from the UK's own summary of its law) that:

> Similarly to what is provided in Article 89 GDPR, personal data processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes can also be exempted from a number of listed provisions of the UK GDPR.
>
> As regards research and statistics, **exemptions are possible** to the provisions of the UK GDPR related to confirmation of processing, access to data and **safeguards for third country transfers**; right to rectification; restriction of processing and objection to processing. As regards archiving in the public interest, exemptions are also possible to

[9] For details, see: ORG, Submission to the European Commission, the European Data Protection Board and the European Parliament on the UK immigration exemption, 3 March 2021, available at: https://www.openrightsgroup.org/publications/submission-to-the-european-commission-and-the-european-data-protection-board-on-the-operation-of-the-uks-immigration-exemption-in-the-data-protection-act-2018/

> the notification obligation regarding rectification or erasure of personal data or restriction of processing and to the right to data portability.
>
> According to paragraphs 27(1) and 28(1) of Schedule 2 to the DPA 2018, the exemptions to the listed provisions of the UK GDPR are possible where the application of the provisions would "prevent or seriously impair the achievement" of the purposes in question.
>
> (recitals 73 – 74, emphases added, footnotes omitted)

What the Draft Decision fails to note is that Article 89(2) and (3) of the EU GDPR does not allow for derogations from the safeguards for third country transfers.

This is not some minor matter. International transfers of data used for research purposes raise many serious data protection issues. It would appear that under the UK GDPR the UK authorities can introduce special derogations from the data transfer rules to allow data transferred from the EU/EEA to the UK to be further transferred (onwardly transferred) to third countries that have not been held to provide adequate/essentially equivalent protection by the EU, for research purposes, without the data exporters and importers having to adopt the kinds of "appropriate safeguards" that must be adopted for transfers of personal data to such countries for such purposes from the EU/EEA itself. This may have implications in particular (but not only) in relation to transfers of lightly pseudonymised data for research purpose (cf. the relaxed UK rules on data sharing, note above, at 1).

This is another area – and an important one – in respect of which the UK therefore manifestly does not provide "essentially equivalent" protection to the EU. But also another one that the Commission failed to note.

3. Data transfer issues

3.1 Transfers and transits (what is a transfer?) (recital 196):

In a sub-section in the section on *Access and use of personal data transferred from the European Union by public authorities in the United Kingdom* (section 3),[10] the Commission (again presumably using text from the UK Government) says that:

> **[the collecting of communications data] by telecommunication operators in the UK directly from the users of a telecommunication service [including from users in the EU: see below] … does not involve a transfer on the basis of this Decision, i.e. a transfer from a controller/processor in the EU to a controller/processor in the UK.**
>
> (recital 196)

This is expanded on in yet another footnote (footnote 316), where the Commission writes, in relation to the retention and acquisition of communications data by UK authorities under the Investigatory Powers Act 2016 (further discussed at II.1, below), that :

> obligations under the IPA 2016 cannot be imposed on telecommunications operators whose equipment is not in or controlled from the UK and who do not offer or provide services to persons in the UK … **If EU subscribers (whether located in the EU or in the UK) made use of services in the UK, any communications in relation to the provision**

[10] Specifically, sub-section 3.3.1.1.2 *Targeted acquisition and retention of communications data*.

> **of this service would be collected directly by the service provider in the UK rather than subject to a transfer from the EU.**

This is remarkably in line with the view taken by the UK ICO in relation to international transfers, i.e., that:[11]

> **Transfer does not mean the same as transit.** If personal data is just electronically routed through a non-UK country but the transfer is actually from one UK organisation to another, then it is not a restricted transfer [i.e., a transfer in relation to which appropriate safeguards must be put in place].
>
> (emphasis added)

The ICO gives the following example:

> Personal data is transferred from a controller in the UK to another controller in the UK via a server in Australia. There is no intention that the personal data will be accessed or manipulated while it is in Australia. Therefore there is no restricted transfer."

Of course, the same would apply if for Australia one would read the USA (or Russia or China).

This is a dangerous new line of reasoning, not underpinned by any EU law or case-law, and relevant also beyond the specific context (which is why it is discussed here). It rests on a semantic point: that routing data from one place or one IT system to another constitutes mere "transiting" but not a "transfer", even if the different places or systems are in different countries. The Commission reasoning similarly seems to rest on the idea that if a controller in one country collects data directly from a data subject in another country (or to be more precise, from a device associated to such a data subject), that also does not constitute a "transfer". **This directly conflicts with the view of the EDPB which stresses that:**[12]

> **remote access by an entity from a third country to data located in the EEA is also considered a transfer.**
>
> (emphasis added)

There are three issues with this. First of all, there is the semantic point: what is the difference between a "transit" and a "transfer"? Is there a difference? Secondly: how does this translate to the realities of global communication systems? And third: what are the implications of this new line of thinking (if accepted) for the application of the EU GDPR and the UK GDPR?

In plain English there is no real distinction between a "transit" and a "transfer". According to the Concise Oxford Dictionary, the verb "**[to] transfer**" means:

> [to] convey, remove, hand over ([a] thing etc. from [a] person or place to another)

The noun "**[a] transfer**" accordingly means:

---

[11] ICO, *International transfers after the UK exit from the EU Implementation Period*, available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/
The issue is discussed in a blog article by me of 2 February 2021, at: https://www.ianbrown.tech/2021/02/02/uk-adequacy-international-transfers-and-human-rights-compliance/

[12] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, adopted on 10 November 2020, footnote 22 (reflected in a range of guidance including on direct access by authorities in third countries to data in the EU/EEA).

> transferring or being transferred; conveyance of property or right [or, one may add, data]

And "**transit**" means:

> going, conveying, being conveyed, across or over or through

If anything, the term "transit" is more related to places while "transfer" can also relate to persons (one can transfer a right without having to move). But there is no semantic basis for distinguishing between "transits" and "transfers" in terms of the GDPR: if data are moved from one country to another – or are made accessible from another country than the one in which they are held – then that constitutes an international data transfer irrespective of whether the data are only routed from one place or one IT system to another in this context, or are collected directly by an entity in one country from the data subjects in another country. The point is that the data are moved from one country to another: that is, in plain language, a cross-border transfer. Moreover, there is nothing in either the text of the GDPR, or its recitals (or as far as I know in any of the *travaux préparatoire*) that suggest that the term (international) transfer must be given a different, technical-legal meaning in that instrument that differs from the ordinary meaning of the term. And:

> Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met.
>
> (Recital 115, reflected in Chapter V GDPR)

The words "routing" and "transit" are not mentioned in either the GDPR itself or the recitals.

In other words, this playing with words is an attempt to exclude "simple routing of data" through third countries and "direct collecting of personal data" by third country entities (private and public) directly from data subjects in the EU/EEA from the rules in the GDPR on international transfers – and onward transfers.

This is in spite of the fact that data routed through third countries (unless fully end-to-end encrypted) or directly obtained from EU persons by entities in third countries are of course susceptible to being accessed by authorities in the relevant third countries – and unduly accessed there by such authorities if the law on such access in such countries is not "essentially equivalent" to EU law and does not conform to the requirements set by the CJEU or by the EDPB in its "European Essential Guarantees for surveillance".

If the UK and EU Commission views were to be allowed to pass, that would drive a coach and horses through *Schrems II*, *PI*, *LQDN* and other judgments, and through the EDPB's EEGs.

Secondly, this risk is especially great in relation to international communications and the provision of e-comms infrastructure including traditional landline and mobile phone services, VoIP, Zoom "meetings", email communications and the routing of data to servers in other countries. The Draft Decision appears to be somewhat ignorant of the global electronic communications infrastructure. Modern electronic communications anywhere, even if seemingly purely domestic, flow through an extremely complex, and extremely integrated global series of cables and nodes and servers, controlled by a range of closely inter-related companies and state entities and intricately connected private and state assets.

It is no longer the case that (say) UK communication service providers collect data from their UK subscribers through infrastructure in the UK controlled by the specific provider: that is an

almost antediluvian view of communication systems. Rather, all of the above types of e-comms data flow through any or all of the different systems, controlled by a wide range of entities (who have complex technical inter-operability and inter-billing arrangements in place to cover this).

In that respect, the attempt by the UK and the Commission to exclude from the protection of the GDPR (or at least from Chapter V) (i) personal data on "*EU subscribers (whether located in the EU or in the UK) [who] ma[k]e use of services in the UK*" and whose data is "collected directly" from them (or rather, their devices) by the UK service provider and (ii) personal data routed through or sent to servers in third countries (including Australia and the USA) **seriously undermines EU data protection** (not least in relation to access to the transferred data by third country agencies). It also undermines the stipulation in Article 3(2)(a) that the GDPR applies (in full) to any non-EU/EEA provider offering their goods or services to individuals in the EU/EEA. Rather, it suggests that such providers can ignore the requirement that "appropriate safeguards" must be put in place in relation to the directly collected data on EU persons.

This is a dangerous line of reasoning that the EDPB and the EP should reject in the strongest terms.

I will discuss the implications in the more specific contexts of onward transfers of personal data on the basis of UK-issued adequacy decisions (sub-section 3.2, below) and to the USA under the UK-US Agreement (sub-section 3.3, below) and of access to personal data on EU persons by the UK intelligence agencies (working hand in glove with their US counterparts) (section II.5, below).

3.2 (Onward) transfers on the basis of UK-issued adequacy decisions (recitals 75 – 82):

The Commission says that the regime for transfers of personal data from the UK to other third countries (which constitute "onward transfers" under the EU GDPR if the data were originally transferred from the EU/EEA to the UK) "*mirrors the one set out in Chapter V of [the EU GDPR]*" (recital 75). One aspect of this is that the UK Secretary of State can issue "adequacy regulations" that are largely similar to the EU GDPR adequacy decisions.

The Draft Decision says that:

> When assessing the adequacy of the level of protection, the Secretary of State must take into account the same elements that the Commission is required to assess under Article 45(2)(a)-(c) of Regulation (EU) 2016/679, interpreted together with recital 104 of Regulation (EU) 2016/679 and the retained EU case law. This means that, when assessing the adequate level of protection of a third country, the relevant standard will be whether that third country in question ensures a level of protection "essentially equivalent" to that guaranteed within the United Kingdom.
>
> (recital 77)

However, as explained in General Comment 3, above, in this respect the UK's highest courts can already depart from the "retained" case-law, including *Schrems II*, *PI* and *LQDN* – and will in any case not be bounds by the judgments in a series of pending cases. UK law says third countries should only be declared to provide adequate protection for personal data if they provide protection that is "essentially equivalent" to the protection accorded by the UK GDPR – but the UK authorities and courts can begin to take different views of what "essential

equivalence" in this regard means, e.g., in relation to access to transferred data by the authorities of the third country in question the UK Secretary of State is not bound by the EU (i.e., the European Commission) views on adequate/essential equivalence with the EU GDPR.

The Draft Decision also says that:

> [P]aragraph 4 of Schedule 21 to the DPA 2018 (introduced by the DPPC Regulations) provide [*sic*] that as of the end of the transition period, certain transfers of personal data are treated as if they are based on adequacy regulations. These transfers include transfers to an EEA State, Gibraltar, a Union institution, body, office or agency set up by, or on the basis of the EU Treaty, and third countries which were the subject of an EU adequacy decision at the end of the transition period. Consequently, the transfers to these countries can continue as before the UK's withdrawal from the EU.
>
> (recital 82, emphasis added)

If the UK were to provide adequate/essentially equivalent protection to personal data compared to the EU, onward transfers of personal data transferred from the EU/EEA to the UK and then back to any EEA State, or to any EU institution or third country that is the subject of an in-force EU adequacy decision would of course not be problematic. However, the Draft Decision fails to point out that this is not what the law says.

In particular, it would appear clear that the UK will regard all non-EU/EEA countries that are recognised by the EU as providing adequate protection on 1 January 2021 as adequate in terms of UK law, pending a review in 2024 – irrespective of what may happen between now and then in respect of those countries in the EU. In that regard, it should be noted that the EU is currently reviewing all previous/current adequacy decisions (as it is required to do under the GDPR). There are serious doubts as to whether a number of them should be allowed to continue: in relation to Canada and New Zealand (as in relation to the UK) similar issues arise in relation to surveillance as led to the invalidating of the Privacy Shield adequacy decision on the USA: they are part of the "5EYES" global surveillance arrangements exposed by Edward Snowden. If those issues stand in the way of a UK adequacy decision (as they should), this should also mean the adequacy decisions on Guernsey, Jersey and the Isle of Man should be seriously reconsidered.[13] And the 2011 adequacy decision on Israel was seriously flawed even in its own terms at the time, and did not take into account the similar surveillance issues that arise there.

Yet it is unthinkable that the UK would not hold the other "British Isles" (Guernsey, Jersey and the Isle of Man) to be "adequate" ("essentially equivalent" to the UK). If proof were needed, the UK has already held **Gibraltar** to provide adequate protection even though there is no EU adequacy decision in place in relation to that territory – a matter which the Commission notes in the above quote, but which for some reason it did not feel worthy of comment. It is widely expected that the UK will include data flows (including personal data flows) in its much hoped-for trade agreement with the USA (even though the EU has strong "horizontal" policies against the inclusion of personal data in such agreements).

---

[13] See Douwe Korff and Ian Brown, Submission to EU re UK adequacy, Executive Summary (discussion of the implications for the UK, other third countries and the EU), 30 November 2020, available at: https://www.ianbrown.tech/wp-content/uploads/2020/11/Korff-Brown-Submission-to-EU-re-UK-adequacy-ExecSumm-DK-IB201130.pdf

Unless there are watertight assurances from the UK Government that it will not declare any non-EU/EEA country to provide adequate protection under the UK GDPR unless that country is also held by the EU to provide adequate protection under the EU GDPR, and that it will suspend or withdraw any UK-issued adequacy decision on any country in respect of which the EU invalidates, suspends or withdraws its adequacy decision, the UK will become a data protection-evasion haven for personal data from the EU/EEA to countries that are not held to provide adequate protection by the EU (or in respect of which a previous decision was invalidated, suspended or revoked), including the other "5EYES" countries (USA, Canada, New Zealand and Australia).

The Draft Decision provides no assurances to that effect.

3.3 <u>(Onward) transfers of personal data to the USA under the UK-US Agreement (recitals 151 – 154):</u>

As the Draft Decision says:

> [S]pecific forms of onward transfers from the United Kingdom to the United States could in the future take place based on 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 (**the "UK-US Agreement"** or "the Agreement"), concluded in October 2019. While the UK-US Agreement has not yet entered into force [at the time of adoption of this Decision], its foreseeable entry into force may affect onward transfers to the US of data first transferred to the UK on the basis of the Decision. More specifically, **data transferred from the EU to service providers in the UK could be subject to orders for the production of electronic evidence issued by competent US law enforcement authorities and made applicable in the UK under this Agreement once in force.** For these reasons, the assessment of the conditions and safeguards under which such orders can be issued and executed is relevant to this Decision.
>
> (recital 151, original text in square brackets, emphases added, footnotes omitted)

As the Draft Decision also points out, in a footnote (footnote 221):

> This is the first agreement reached under the US Clarifying Lawful Overseas Use of Data (CLOUD) Act … that clarifies … that U.S. service providers are obliged to comply with U.S. orders to disclose content and non-content data, regardless of where such data is stored. The CLOUD Act also allows the conclusion of executive agreements with foreign governments, on the basis of which U.S. service providers would be able to deliver content data directly to these foreign governments.

The main reason why the Commission feels this UK-US Agreement does not stand in the way of an adequacy decision (also not as and when it comes into force) is that:

> [D]ata obtained under this agreement benefits from **equivalent protections to the specific safeguards provided by the so-called "EU-US Umbrella Agreement** – a comprehensive data protection agreement concluded in December 2016 by the EU and the US and that sets out the safeguards and rights applicable to data transfers in the area of law enforcement cooperation – which are all incorporated into this Agreement by reference on a *mutatis mutandis* basis to notably take into account the specific nature of the transfers (i.e. transfers from private operators to a law enforcement [*sic*], rather than transfers between law enforcement authorities. The UK-US Agreement specifically provides that equivalent protections to those provided by the EU-US

> Umbrella Agreement will be applied "to all personal information produced in the execution of Orders subject to the Agreement to produce equivalent protections".
>
> **Data transferred to US authorities under the UK-US Agreement should therefore benefit from protections provided by an EU law instrument, with the necessary adaptations to reflect the nature of the transfers at issue.** The UK authorities have further confirmed that the protections of the Umbrella Agreement will apply to all personal information produced or preserved under the Agreement, irrespective of the nature or type of body making the request (e.g. both federal and State law enforcement authorities in the US), so that equivalent protection must be provided in all cases. However, the UK authorities have also explained that **the details of the concrete implementation of the data protection safeguards are still subject to discussions between the UK and the US.** In the context of the talks with the European Commission's services on this decision, **the UK authorities confirmed that they will only let the Agreement enter into force once they are satisfied that its implementation complies with the legal obligations provided therein, including clarity with respect to compliance with the data protection standards for any data requested under this Agreement.** As a possible entry into force of the Agreement may impact the level of protection assessed in this Decision, **any future clarification regarding the way the US will comply with its obligations under the Agreement should be communicated by the UK to the European Commission, as soon as it becomes available, to ensure proper monitoring of this decision** in line with Article 45(4) of Regulation (EU) 2016/679. Particular attention will be given to the application and adaptation of the Umbrella Agreement's protections to the specific type of transfers covered by the UK-US Agreement.
>
> More generally, **any relevant development as regards the entry into force and application of the Agreement will be duly taken into account in the context of the continuous monitoring of this decision**, including with respect to the necessary consequences to be drawn in case of any indication that an essentially equivalent level of protection is no longer ensured.
>
> (recitals 152 – 154, emphases added, footnotes omitted)

This is far from reassuring. First of all, European civil society, academics and Members of the European Parliament had – and still have – serious reservations about the EU-US Umbrella Agreement. Many – including the author of this note – believe it does not ensure "essentially equivalent" protection to personal data compared with the EU instruments. They will be equally concerned about the "equivalent" protections to the EU-US Umbrella Agreement in the UK-US Agreement. Moreover, there is no guarantee that even the (in their view, defective) safeguards in the Umbrella Agreement will be fully applied under the UK-US Agreement: they are to be applied "*mutatis mutandis*", with "*adaptations to reflect the nature of the transfers at issue*". The only assurance in that respect is that "they" – i.e., the UK authorities – will satisfied themselves that the implementation of the UK-US Agreement "*complies with the legal obligations provided [in it]*".

There are also no real safeguards in the requirement that the UK Government should inform the EU Commission of "*any future clarification regarding the way the US will comply with its obligations under the Agreement*", with the Commission then taking this future clarification into account in its continuous monitoring of the UK adequacy decision. Not only does this leave it to the UK to decide what it should or should not tell the Commission in this regard – it also relies on the seriousness of this "continuous monitoring" of adequacy decisions by the

Commission. As will be noted at III, below, to date this supposed "continuous monitoring" by the Commission has been abysmal.

In the circumstances, the acceptance by the Commission of the UK-US Agreement fundamentally undermines the soundness of the adequacy decision.

3.4 Compliance with foreign judgments and orders (recital 76):

Article 48 GDPR stipulates in relation to "*[t]ransfers or disclosures not authorised by Union law*" that:

> Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

The Draft Decision refers to this, somewhat surprisingly, only in a footnote (footnote 78, to recital 76), as follows:

> [T]he United Kingdom has chosen not to include [Article 48 of Regulation (EU) 2016/679] in the UK GDPR. **The UK authorities have explained that they did not consider necessary to introduce such a provision clarifying that requests to transfer data to a third country from a court or an administrative authority of that third country are enforceable only if an international agreement to that effect exists with the country in question, given that the UK legal order already provides sufficient safeguards in that respect.** First, in order to enforce a foreign judgment, courts in the United Kingdom need to be able to point to common law or to a statute that allows its enforceability. However, according to the UK authorities, neither common law nor statutes provide for the enforcement of foreign judgments requiring the transfer of data without an international agreement in place. **As a consequence, requests for data are unenforceable and a provision such as Article 48 of Regulation (EU) 2016/679 would have no legal added value under United Kingdom law.** Second, the United Kingdom authorities have explained that any transfer of personal data to third countries – including if upon request from a foreign court or administrative authority – remains subject to the restrictions in Chapter V of the UK GDPR and therefore requires a transfer tool such as an adequacy regulation or appropriate safeguards, unless one of the derogations in Article 49 of the UK GDPR applies.
>
> (emphases added)

This is somewhat surprising, since the UK originally gave a different reason for not incorporating Article 48 GDPR (Article 43a as it then was in the draft GDPR) into UK law, i.e., that this was judicial cooperation clause and the UK had opted out of the EU judicial cooperation arrangements by means of a protocol to the Lisbon Treaty.[14]

Given the importance of Article 48 to the European Parliament in particular (it having been included in the GDPR at Parliament's insistence), this would have deserved closer analysis.

[14] See the statement made by the Parliamentary Under-Secretary of State at the Department for Business, Innovation and Skills, Baroness Neville-Rolfe, to the UK Parliament on 4 February 2016 (Statement UIN HLWS500), available at:
https://questions-statements.parliament.uk/written-statements/detail/2016-02-04/HLWS500

For instance, the third and fourth sentences in the quote refers to enforcement of foreign judgments through the UK courts – which of course will have to be based on an international agreement (in particular, a Mutual Legal Assistance Treaty, MLAT). But Article 48 refers mainly to compliance with a foreign judgment or administrative order by an EU-based corporate entity – and by extension, of a UK-based corporate entity – without a court being involved.

It has to be admitted that the relationship between Article 48 GDPR and the remainder of Chapter V, in particular Articles 46 and 49, is unclear. But it was clearly the intention of the EU legislator (in particular the EP) that Member States should bar companies under their jurisdiction from meekly complying with judgments and orders from non-EU Member States; that the same should apply in relation to onward transfers from third countries; and that that should be reflected in all adequacy decisions.

The final sentence in the quote above makes clear that the UK effectively wants to ignore and bypass that constraint – and that the Commission is willing to collude in that.

4. Oversight and enforcement by the ICO (recitals 85 – 98):

Some years ago, I analysed the enforcement policies and actions of the ICO for the EU Fundamental Rights Agency, and concluded as follows:[15]

> [E]nforcement of data protection in the UK is 'soft': most cases are not even assessed with a view to determining if the law was breached; Information- and Enforcement Notices are very sparingly used even in cases in which it is found that a breach of the law was 'likely'; and prosecutions are initiated in only a minute fraction of all cases in which there was a criminal breach of the Act. Rather, most cases that are assessed end in a 'negotiated resolution'. There is little insight into the terms on which these negotiations are settled - which raises serious doubts about both the acceptability of such settlements and the specific application of the law (and the Directives) in the UK.

This was some time ago and it appears that enforcement has improved – although it tends to still focus on a few highly publicised cases, with overall enforcement remaining "soft".

This appears to be confirmed by the Draft Decision, although again in a footnote, without critical analysis. The Commission notes, in recital 96, that:

> Since the introduction of Regulation (EU) 2016/679, the ICO handles about 40,000 complaints from data subjects per year and, in addition, carries out about 2,000 ex officio investigations.

A footnote to this paragraph (footnote 104) provides some basic statistics:

> According to the information provided by the UK authorities, during the period covered by the Information Commissioner's Annual Report 2019-2020:
>
> - no infringement was found in about 25% of the cases;

---

[15] Douwe Korff, Thematic Study on assessment of data protection measures and relevant institutions [United Kingdom], February 2009, country report produced for a project commissioned by the EU Fundamental Rights Agency, Executive Summary, para. 25, available at: https://fra.europa.eu/sites/default/files/role-data-protection-authorities-2009-uk.pdf
For the detailed analyses and statistics, see section 2.2.7, *The use of the ICO's powers in practice – a critical assessment*.

- in about 29% of the cases the data subject was asked to either raise the concern with the data controller for the first time, to wait for the controller's reply or to continue an ongoing dialogue with the data controller;
- in about 17% of the cases, no infringement was found but advice was provided to the data controller;
- **in about 25% of the cases the Information Commissioner found an infringement and either provided advice to the data controller or the data controller was required to take certain actions;**
- in about 3% of the cases it was determined that the complaint did not fall under Regulation (EU) 2016/679; and
- about 1% of the cases were referred to another data protection authority in the framework of the European Data Protection Board.

(indents and emphasis added)

In fact, the percentage of cases in which the Commission found an infringement is higher than the "25%" suggested, because the 100% on which that is based includes the 29% of cases in which the ICO told the data subject to raise the concern with the controller or wait for the latter's reply, the 3% that fell outside of the GDPR and the 1% of cases referred to other supervisory authorities. Those cases, in which the ICO did not examine the merits of the case, amount to 33% of all cases. Of the cases that fell within the scope of the GDPR and that were not referred to other supervisory authorities and that were actually looked at by the ICO (the remaining 67% of the 40,000), the corrected statistics are as follows (approximates):

-	Total number cases looked at: 67% of 42.000			= ± 28.000
-	No infringement:	25% of 40.000	= ± 10.000	= ± 35% of 28.000
-	"Advice":	17% of 42.000	= ± 7.000	= ± 25% of 28.000
-	Infringement:	25% of 40.000	= ± 10.000	= ± 35% of 28.000

In other words, in about ten thousand cases – a third of all cases looked at (the vast majority on the basis of a complaint) – the ICO found that the law had been broken ("infringement").

Yet it is still startling to see the results in terms of action taken (of which the Draft Decision notes only the 22 penalty notices under the DPA 1998):[16]

- 1421 decision notices (informing a complainant of the outcome of the ICO assessment), of which:
  - 465 upheld the complaint;
  - 271 partially upheld the complaint; and
  - 685 rejected the complaint.
- 22 penalty notices;

[16] The statistics relate to the year 2018-19, as reported in the ICO Annual Report on that year (to which the Commission also refers in footnote 107). The numbers for decisions notices are given on p. 58; the numbers for penalty notices and information notices are given on p. 24; the other numbers are given on p. 23. The report says that "*We [the ICO] have also taken significant action through enforcement notices, particularly in two priority investigations*" – but there is no information on any other enforcement notices, so presumably there were only these two.

- 11 formal assessment notices;
- An unclear number of "No-notice" assessment notices;
- 11 information notices;
- 2 enforcement notices;

In other words, while the ICO looked at about 28.000 cases, and while there were approximately 10.000 cases in which the ICO found that the law had been broken, complaints were only formally "upheld" in about 730 cases (<3%), and there was only serious, "hard" enforcement in 24 cases (in the form of 22 penalty notices and 2 enforcement notices issued), i.e., in less than 0.025%.

Given these statistics, it is difficult to see how the ICO can be said to have met the "procedural and enforcement mechanisms" requirement set out in the WP29 (EDPB-endorsed) Adequacy Referential, that stipulates that (for an adequacy decision to be issued):

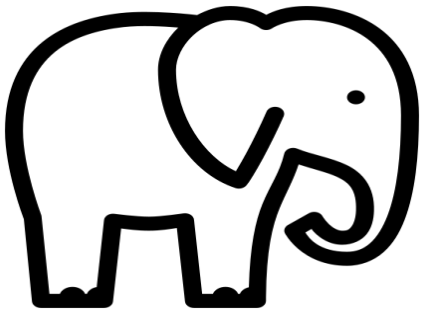
> **The data protection system must provide support and help to individual data subjects in the exercise of their rights and appropriate redress mechanisms.**
>
> The individual should be able to pursue legal remedies to enforce his/her rights rapidly and effectively, and without prohibitive cost, as well as to ensure compliance. To do so **there must be in place supervision mechanisms allowing for independent investigation of complaints and enabling <u>any infringements of the right to data protection and respect for private life to be identified and punished in practice</u>.**
>
> **Where rules are not complied with, the data subject should be provided as well with effective administrative and judicial redress**, including for compensation for damages as a result of the unlawful processing of his/her personal data. This is a key element **which must involve a system of independent adjudication or arbitration which allows compensation to be paid and <u>sanctions imposed</u> where appropriate.**
>
> (WP29 Adequacy Referential (WP254rev01), section C.4, emphases added)

It is difficult to see how the Commission – had it looked at the above statistics – could have concluded that the ICO "identifies and punishes" transgressors "in practice" and "imposes [appropriate] sanctions" on controllers and processors who break the law. In fact, on the contrary, the ICO noticeably continues to fail to properly enforce the law in the vast majority of cases – even when it itself concludes that the law has been broken.

- o – o – o -

II. Issues relating to UK national security and bulk surveillance powers[17]

1. The elephant in the room:



Korff-Brown factual findings as to the UK surveillance practices (summarised):

- The UK, working jointly with the US National Security Agency (NSA), taps into a large number of selected Internet communications link (especially but not only underseas cables), including cables through which most of the communications of EU individuals, institutions and officials travel (in particular, most EU – UK – USA communications). These communications include not only emails and social media exchanges but also the data flows between EU users of US-based cloud services and the relevant US cloud servers.
- Very large amounts of data – including all communications metadata (including traffic and location data) are extracted by the UK from all selected bearers indiscriminately, in bulk, and retained for some time.
- The metadata are highly revealing of the lives of potentially hundreds of thousands of individuals to which they may relate, but the vast majority of data subjects to which the metadata relate – which for many selected bearers will include large numbers of EU persons – will have no links with terrorism, threats to national security or serious crime.
- While much of the other data are filtered out fairly quickly through "simple" or "complex" queries, the metadata and the not-filtered-out data are retained for longer, to allow for their use in algorithmic analyses and profiling.
- The not-filtered-out data, including all metadata, are subject to automatic analyses by means of self-learning (AI-based) algorithmic datamining, to "identify" (i.e., label) individuals as or linked to "Subjects of Interest" ("SoI") – but this processing suffers from major, unavoidable defects: built-in biases, mathematically unavoidable excessive numbers of "false positives" or "false negatives" (or both), and the fact that because of their complexity they become effectively unchallengeable. It is unavoidable that many individuals who are labelled or linked to "SoI" are innocent and have no links to serious crime or terrorism.

---

[17] This is probably the most contentious issue in relation to UK adequacy. It is examined in some detail in Korff-Brown Submission to EU re UK adequacy, Part Two re UK surveillance, 30 November 2020, available at: https://www.ianbrown.tech/wp-content/uploads/2020/11/Korff-Brown-Submission-to-EU-re-UK-adequacy-Part-Two-DK-IB201130.pdf
At the beginning of section II.1, I therefore quote the relevant factual conclusions from that submission, as summarised in the Executive Summary of both parts of the submission (footnote 13, above). For details of the factual matters relating to surveillance, summarised in the Executive Summary, see Part Two.

After *Schrems II*, the issue of "*access to personal data [transferred from the EU/EEA to a third country] by authorities of the third country*," in particular the third country's intelligence agencies (including direct access to data in the EU/EEA by such authorities or agencies) is a crucial matter to be assessed by the Commission in any adequacy review. The Draft Decision does indeed touch on this issue, but as noted below limits itself to a (not very serious) examination of the law (as described by the UK authorities).

The Draft Decision completely fails to assess (or even note) the UK's intelligence agencies' actual surveillance practices. It does not mention the Snowden revelations, or the US-UK "TEMPORA" programme, or the joint UK-US bulk interception station in Bude, Cornwall, or what it is used for, or the European Parliament's report on US surveillance (which is also extremely relevant to the UK), or Caspar Bowden's report to the EP, or the UK NGO *Open Rights Group*'s excellent and detailed reports into the UK surveillance practices and laws, or Eric King's witness statement on behalf of *Privacy International* in the case before the UK Investigatory Powers Tribunal (or our own summaries of these matters).[18]

The Commission simply does not want to see or hear about or talk about these practices.

The only references as to what may actually be done by the UK intelligence services, and as to whether this may affect EU persons (and, one may add, EU institutions and officials and institutions and officials of EU Member States) are in these two sentences:

> It should be noted that **the retention and acquisition of communications data normally does not concern personal data of EU data subjects transferred under this Decision to the UK**. The obligation to retain or disclose communications data pursuant to Part 3 and 4 of the IPA 2016 covers data that is collected by telecommunication operators in the UK directly from the users of a telecommunication service.
>
> (recital 196, where it also suggested that direct collection of data by a UK provider from users in the EU/EEA does not involve a "transit": see section 3.1, above))
>
> As it is the case for targeted retention and acquisition of communications data (see [para] (196)), also **the bulk acquisition of communications data does normally not concern personal data of EU data subjects transferred under this Decision to the UK**.
>
> (recital 225)

The Commission did not bother to find out in more detail what "**not normally**" means in this regard. But it is reminiscent of the UK authorities claim that GCHQ only chooses to collect data in bulk from only "**a small proportion** of [the bearers within the Internet cables] they can theoretically access".[19]

In other words, the phrase "not normally" is likely to be used to suggest that any collection of personal on EU data subjects in the course of bulk extraction of data from the Internet cables

---

18 In Korff-Brown Submission to EU re UK adequacy, Part Two re UK surveillance (previous footnote).

19 UK House of Commons' Intelligence and Security Committee, Privacy and Security: A modern and transparent legal framework (HC 1075), 12 March 2015 ("the ISC Report"), para. 64, quoted and discussed in Korff/Brown (previous footnote), at p. 11.

makes up only a small portion of the data collected in this way globally, i.e., that GCHQ mainly focusses on other data and data on non-EU individuals (such as people "of interest" in Afghanistan, Syria, Russia or Yemen). The UK – and, it would appear, the Commission – are effectively saying: "*surveillance of EU persons is only a very small part of the UK-US massive global surveillance operations, and not worth bothering about.*"

It may well be true that UK (and UK-USA/5EYES) surveillance is mainly focussed outside the EU/EEA. But the sentences quoted still confirm that the UK does collect personal data on EU data subjects. The fact that they collect much more data on non-EU persons is irrelevant to that and certainly not as such an excuse for the operations in which data on EU persons is collected.

Hopefully, the EDPB and the EP will seek further details on this issue – and will not accept that it can be ignored because it "does not happen normally" or all that often (comparably speaking).

The Commission's summaries of the law, discussed in the following sections, should be assessed in the light of the express acknowledgement that bulk acquisition of personal data on EU persons does occur. In those sections, I will also note that the Commission nowhere clearly and specifically assessed the legal rules it described against the applicable standards.[20]

2. The national security exemption (recitals 124 – 130):

The Draft Decision notes that "*Section 110 of the DPA 2018 provides for an exemption from specified provisions in Part 4 of the DPA [that applies to processing by or on behalf of the UK intelligence services] when such exemption is required to safeguard national security*" (recital 125). The "specified provisions" include, in particular, data subject rights.

In theory, any UK authorities relying on this exemption must decide on a case-by-case basis if it is really necessary to rely on the exemption for this purpose. But the DPA also provides for the issuing of a certificate by a Cabinet Minister or the Attorney General certifying that a restriction of the relevant rights is a necessary and proportionate measure to the protection of national security. The certificate "***is conclusive evidence of that fact***" (i.e., that the restriction of the rights of the relevant data subject is necessary for national security) (S. 111(1)).

The Draft Decision makes two points in relation to this. On the one hand, it says that:

> Whether or not the exemption has been used appropriately is subject to the oversight of the ICO (recital 125, last sentence)

On the other hand, it says in a footnote (footnote 172) that:

> According to the explanation provided by the UK authorities, while a certificate is conclusive proof that, in respect to data or processing described in the certificate, the exemption is applicable, it does not remove the requirement for the controller to consider whether there is a need to rely on the exemption on a case-by-case basis.

[20] Cf. General Comment 2, above. For an overview of those applicable standards in this area, see Korff-Brown Submission to EU re UK adequacy, Part Two re UK surveillance (footnote 17, above), section 3.1.2, *Main issues and applicable standards*.

In this respect, the Draft Decision refers to a Memorandum of Understanding (MoU) between ICO and UKIC according to which:

> Upon the ICO receiving a complaint from a data subject, the ICO will want to satisfy themselves that the issue has been handled correctly, and, where applicable, that the application of any exemption has been used appropriately.
>
> (Memorandum of Understandings between Information Commission's Office and the UK Intelligence Community, paragraph 16, available at the following link: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf)

The way in which this paragraph is quoted in the Draft Decision suggests that the ICO has competence and jurisdiction to rule on the matter – on whether a complaint has been handled correctly by the intelligence services and on whether they were right to rely on the exemption.

But a closer look at the MoU suggests otherwise, at least in relation to access requests:

> Should ICO caseworkers request an explanation for the response made by a UKIC Agency, the response will be provided to the ICO within 20 working days. Where the UKIC Agency requires this to be classified as SECRET or above it will need to be appropriately secured at the ICO premises, or stored on the ICO's behalf at UKIC premises. The classification of the response will depend on the circumstances of each case and where appropriate will include a general description of the searches carried out and whether the national security exemption has been relied upon (whether by a Neither Confirm Nor Deny (NCND) response or refusal). If personal data is held, where applicable, the UKIC Agencies will state in broad terms why any exemption has been applied and why the material cannot be released (for example it relates to a covert investigation or operation, or it would impair UKIC operations). If an NCND response is given then a similar statement describing why this is necessary will be provided.
>
> If the matter is particularly sensitive, the ICO will ensure the Case is transferred to a senior ICO member of staff with appropriate Developed Vetting clearance, and that all further communications are made through secure means, if available. Alternatively, the ICO will be briefed at UKIC Agency premises.
>
> The UKIC Agency response will be held securely and in confidence by the ICO, and not communicated to the data subject. If the UKIC Agency relies on an NCND response, and the ICO is satisfied with this approach, the ICO will not reveal to the data subject whether personal data is held.
>
> (paras. 17 – 19)

This suggests that while the ICO may express views on whether they feel the exemption has been properly relied upon or not, the ICO cannot instruct the relevant agency to act differently. And if the intelligence agency decides that the data subject should be kept completely in the dark (i.e., not even told whether the agency hold data on him or her, let alone what data), there does not appear to be anything the ICO can do about that – it must follow such "Neither Confirm Nor Deny [NCND]" response. At most, if the ICO is "not satisfied" in this respect, it can inform the relevant agency of this view.

This may be justified in this sensitive area – but it is misleading to say that the intelligence agencies are, in the use of the exemption, subject to any real, meaningful "oversight" by the ICO.

Judicial review is also limited, especially in relation to national security matters. First of all, as already noted in General Comment 5, above, such review is generally limited to questions of illegality, procedural unfairness and irrationality (and likely to be further limited in future). Given the broad phrasing of the national security exemption, the first ground is of limited value, especially against a "conclusive" certificate, and a Secretary of State will normally also follow the procedural rules correctly. Which leaves "irrationality" – a very high bar to overcome. But in relation to national security issues that bar is raised even higher – as was made clear in a judgment of the UK Supreme Court issued at the very time this note was being finalised. In a ruling on an appeal from an ISIS follower whose British nationality had been revoked, the Supreme Court ruled that:[21]

> [T]he Court of Appeal erred in its approach [when it] made its own assessment of the requirements of national security, and preferred it to that of the Home Secretary, despite the absence of any relevant evidence before it, or any relevant findings of fact by the court below. Its approach did not give the Home Secretary's assessment the respect which it should have received, given that it is the Home Secretary who has been charged by Parliament with responsibility for making such assessments, and who is democratically accountable to Parliament for the discharge of that responsibility.

The requirement that the UK courts should show "respect" and deference to the Government on matters relating to national security makes clear that judicial review of such matters is marginal at most: only if clear evidence is available to a UK court that shows that a minister's views on a national security matter are unsustainable ("irrational") will the court set a decision in this area aside. That falls far short of judicially applied tests of necessity and proportionality.

This raises doubts about the Commission's conclusion in the Draft Decision that:

> It follows from the above that limitation [*sic*] and conditions are in place under the applicable UK legal provisions, as also interpreted by the courts and the Information Commission, to ensure that these exemption and restrictions remain within the boundaries of what is necessary and proportionate to protect national security.

In fact, neither the legal provisions (presumably, SS. 110 and 111 DPA) nor the ICO-UK Intelligence Community MoU "ensure" that the exemption is only used when objectively necessary and proportionate to protect national security. They place an obligation on the part of the authorities issuing a "conclusive" certificate to consider the necessity and proportionality of the certificate – but do not involve effective substantive oversight by the ICO or the courts to ensure this is properly done.

This raises doubts about the compatibility of the law with fundamental (EU CFR) requirements.

[21] UK Supreme Court judgment in *R (on the application of Begum) (Appellant) v Special Immigration Appeals Commission (Respondent) R (on the application of Begum) (Respondent) v Secretary of State for the Home Department (Appellant) Begum (Respondent) v Secretary of State for the Home Department (Appellant)*, [2021] UKSC 7 on appeal from: [2020] EWCA Civ 91826, February 2021, para. 134, available at: https://www.supremecourt.uk/cases/docs/uksc-2020-0156-judgment.pdf

3. Limitations on the use of the UK "bulk powers" (recital 211ff.):

The Draft Decision raises the semantic issue of whether the (acknowledged) "*collection and retention of large quantities of data acquired by the Government through various means (i.e. the powers of bulk interception, bulk acquisition, bulk equipment interference and bulk personal datasets)*" (collectively referred to as "**bulk powers**") and the subsequent accessing of the data by the UK authorities constitutes "**mass surveillance**" – and concludes that it does not, because it is not done "*without limitations or safeguards*" (recital 211). This is a similar (and similarly unproductive) discussion as the one in the UK as to whether the bulk collection is "targeted" or "indiscriminate".[22]

The real issue is whether the bulk powers are used in accordance with the principles established in the CJEU *Schrems II* judgment and the EDPB's European Essential Guarantees for surveillance.

In that respect, the Draft Decision discusses at some length the various limitations that are in place – which are mostly of a procedural nature. Thus, the Draft Decision explains in relation to bulk interception and bulk equipment interference in section 3.3.1.1.4.1 that:

- a warrant authorising a bulk interception or a bulk equipment interference may be issued by the Secretary of State only if s/he regards this as "necessary for the interest of national security" (or for the purposes of preventing or detecting serious crime or the interest of the economic well-being of the United Kingdom when relevant for national security) (recital 215);
- a bulk interception warrant must be specified in greater detail than the simple reference to the "interests of national security", the "economic wellbeing of the UK" and of "preventing and combating serious crime" but a link must be established between the measure to be sought and one or more operational purpose/s that must be included in the warrant (*idem*);
- the operational purposes specified in the warrant must be specified in a list maintained by the heads of the intelligence services (recital 216);
- the selection for examination of the material collected under the bulk warrant must be justified in light of the operational purpose/s, and this must be assessed by the Secretary of State (recital 217);
- the use of the bulk powers must be proportionate to the aim pursued (recital 218); and
- the above must be assessed by a Judicial Commissioner using the same principles that would be used by a court in an application for judicial review (recital 220).

There are also time limits (six months renewable) (recital 221) and security requirements (recital 222), and further checks on the proportionality of examination of the data collected in bulk (recital 223).

---

[22] See Korff-Brown Submission to EU re UK adequacy, Part Two re UK surveillance (footnote 17, above), section 2.2.2, at ii (pp. 9 – 13).

Similar procedural requirements are in place in relation to the use of the other bulk powers (see sections 3.3.1.1.4.2 *re* bulk acquisition of communications data and 3.3.1.1.4.3 *re* retention and examination of bulk personal datasets).

The point to be made about this is that all these matters are left to the assessment by the authorities themselves, subject to oversight by the Judicial Commissioner. They intelligence agencies decide what data – or indeed what bearers – may be relevant or necessary or proportionate to collect/access for national security purposes. And although the Judicial Commissioners are senior judicial figures whose integrity is not put in doubt, their scrutiny is clearly in line with what I said earlier, i.e., it is very marginal. This is clearly shown by the statistics on their authorising of refusing proposed warrants. According to the latest annual report of the Investigatory Powers Commissioner, for 2019, for bulk powers the statistics were as follows:[23]

Bulk personal datasets - class warrant:

- considered 101
- approved 101
- *refused 0*

Bulk personal datasets – specific warrant:

- considered 85
- approved 85
- *refused 0*

Bulk communications data acquisition warrant:

- considered 18
- approved 18
- *refused 0*

Bulk interception warrant:

- considered 30
- approved 30
- *refused 0*

Bulk equipment interference warrant:

- considered 10
- approved 10
- *refused 0*

What is more, the Commission failed to assess the above procedural arrangements in the light of the standards which it claimed it would apply: those established by the CJEU and the

[23] Annual Report of the Investigatory Powers Commissioner 2019 (IPCO report), p. 140, available at: https://www.ipco.org.uk/docs/IPC%20Annual%20Report%202019_Web%20Accessible%20version_final.pdf Note that any single warrant can cover many different bearers and thousands of individuals.

European Court of Human Rights and the EDPB in their EEGs. These in particular all agreed that the law "must itself define" the scope and application of any surveillance measure (such as the use of bulk powers):

> [T]he requirement that any limitation on the exercise of fundamental rights must be provided for by law implies that **the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned**.
>
> (CJEU *Schrems II* judgment, para. 175, with reference to its Opinion 1/15 on the EU-Canada PNR Agreement of 26 July 2017, paragraph 139, and other case-law cited; emphases added).

The above is repeated verbatim with a cross-reference in the CJEU's *PI* judgment, para. 65, and in its *LQDN* judgment, para. 175. Cf. also its *DRI* judgment, para. 68 (re EU law), and also in the EDPB's EEGs, para. 36.

In its *Big Brother Watch* judgment, the ECtHR has outlined "six minimum requirements" that surveillance laws must meet in order to ensure that they are "sufficiently foreseeable to minimise the risk of abuses of power" and which can be said to also indicate the "defining" that the CJEU says should be enshrined in the law itself. These are (in summary):

- **[the need for a specification of] the nature of offences which may give rise to an interception order;**
- **[the need for] a definition of the categories of people liable to have their communications intercepted;**
- [the need for] a [stipulated] limit on the duration of interception;
- [the need for an appropriate] procedure to be followed for examining, using and storing the data obtained;
- [the need for appropriate] precautions to be taken when communicating the data to other parties; and
- [the need for limitations on] the circumstances in which intercepted data may or must be erased or destroyed

(ECtHR, *BBW* judgment, para. 423, summarising the more detailed overview of the six requirements in para. 307, with indents, words in square brackets and emphases added. See also the EEGs, para. 30).

The first two of these correspond to the CJEU requirement that there must be some reasonable link between the individuals whose data are collected and the offences or threats to national security in relation to which their data are collected.

In other words: the law itself should expressly preclude the collection of personal data (including metadata) on individuals who have no personal link, or some link in time or place, to the offences or threats in question. General, indiscriminate, "dragnet", bulk collection of personal data (including metadata) – collecting of the "hay" from a "haystack" in order to find a "needle" buried in it – is fundamentally incompatible with EU fundamental rights law; and the laws covering surveillance should themselves, explicitly make clear that such bulk collection is not permitted. This cannot be left to vague language such as instructing a government minister authorising surveillance to do so only in a "proportionate" manner.

The UK law allowing for the use of bulk powers does not in itself, on its face, specify the nature of offences which may give rise to the issuing of a bulk powers warrant (rather, they can be used in relation to any "interests of national security", including the "economic wellbeing of the UK" and "preventing and combating serious crime" when related to national security), and the law also does not, in itself, on its face, define the categories of people on whom data can be collected under the bulk power warrants.

Those matters may well, to some extent,[24] be addressed in the processes concerned – but that is not the same as specifying them in the law itself. That is clearly not in accordance with the case-law of the CJEU and the ECtHR, or with the EDPB's European Essential Guarantees.

Moreover, as noted earlier, the assessment by a Judicial Commissioner "*using the same principles that would be used by a court in an application for judicial review*" of national security-related decisions will suffer from the same limitation as noted in the previous section (as clarified in the *Begum* judgment of the UK Supreme Court): the Commissioners are obliged to be respectful and deferential to the government minister who issues a bulk powers warrant and only oppose it if there is a clear evidence that the warrant is not necessary or proportionate (or to be more precise: cannot rationally be said to be necessary or proportionate)

4. The nature and use of the data obtained in bulk (recitals 223, 233 and 288):

The description of the processing of the bulk data suggests that while large amounts are originally captured, irrelevant material is then quickly filtered out by automated means, with only relevant material "retained and examined":

> [T]he UK authorities clarified that the material intercepted in bulk is selected, first of all, via **automated filtering with the aim to discard data that is unlikely to be of national security interest**. The filters will vary from time to time (as internet traffic patterns, types and protocols change) and will depend on the technology and operational context. After this phase, the data can be selected for examination only if relevant for the operational purposes specified in the warrant.
>
> (recital 223, emphasis added)
>
> Bulk Personal Dataset (BPD) warrants411 authorise intelligence agencies to **retain and examine** sets of data that contain personal data relating to a number of individuals.
>
> (recital 233, emphasis added)

In other words, the focus of the (largely procedural) legal regulation is on data that are retained after initial filtering, and only then "examined", i.e., by an official. The suggestion is that there is only an intrusion into individual privacy and data protection rights if any of the data collected in bulk are retained after filtering and examined by an official, and more specifically that metadata (referred to as "secondary data") are not intrusive:[25]

---

[24] In fact, the level of scrutiny by the Secretary of State is not always as in-depth as the descriptions in section 3.3.1.1.4.1 (*re* bulk interception and bulk equipment interference, summarised above) and section 3.3.1.1.4.2 (*re* bulk acquisition of communications data) suggest. As section 3.3.1.1.4.3 *re* retention and examination of bulk personal datasets) and footnote 417 to that section make clear, the Secretary of State only assesses **in general terms** whether so-called "class BPD warrants", which concern "a certain category of datasets", are "necessary" and "proportionate".

[25] Draft Decision, footnote 288.

> Secondary data are data attached or logically associated with the intercepted communication, can be logically separated from it and if it were so separated, would not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication. Some examples of secondary data include router configurations or firewalls or the period of time a router has been active on a network when they are part of, attached to or logically associated with intercepted communication.
>
> For more details see the definition in Section 16 of the IPA 2016 and Code of Practice on Interception of Communications, paragraph 2.19, see footnote 282.

The above is seriously misleading. This is what the Code of Practice actually says:[26]

> [Bulk interception warrants] may authorise the interception of communications and/or the obtaining of secondary data. A warrant may provide for the obtaining of only secondary data. Secondary data is defined in sections 16 and 137 and comprises:
>
> - **systems data** (as defined in section 263(4)) which is comprised in, included as part of, attached to or logically associated with the communications being intercepted; and
> - **identifying data** (as defined in sections 263(2) and (3)) which is comprised in, included as part of, attached to or logically associated with the communication, which is capable of being logically separated from the remainder of the communication and which, once separated, does not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication.
>
> **Systems data** as defined in section 263(4) means any data that enables or facilitates, or identifies and describes anything connected with enabling or facilitating, the functioning of any systems or services.[27] Examples of systems data would be:
>
> - messages sent between items of network infrastructure to enable the system to manage the flow of communications;
> - router configurations or firewall configurations;
> - software operating system (version);
> - historical contacts from sources such as instant messenger applications or web forums;
> - alternative account identifiers such as email addresses or user IDs; and
> - the period of time a router has been active on a network.
>
> Where systems data is comprised in, included as part of, attached to or logically associated with the intercepted communication then it will fall within the definition of secondary data in sections 16 and 137.
>
> **Identifying data** as defined in sections 263(2) and (3) is data which may be used to identify, or assist in identifying:
>
> - any person, apparatus, system or service;
> - any event; or
> - the location of any person, event or thing

---

[26] Interception of Communications Draft Code of Practice, December 2017, sections 2.19 and 2.20, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/668941/Draft_code_-_Interception_of_Communications.pdf

[27] Systems data that is necessary for the provision and operation of a service or system also includes the data necessary for the storage of communications and other information on relevant systems. Systems data held on a relevant system may be obtained via an equipment interference warrant under Part 5 or Chapter 3 of Part 6 of the Act. [original footnote]

> In many cases this data will also be systems data, however, there will be cases where this data does not enable or otherwise facilitate the functioning of a service or system and therefore is not systems data. Where identifying data is comprised in, included as part of attached to or logically associated with the communication, can be logically separated from the remainder of the communication and does not, once separated, reveal anything of what might reasonably be considered to be the meaning (if any) of any communication (disregarding any inferred meaning) it will fall within the definition of secondary data in sections 16 and 137. Examples of such data include:
>
> - the location of a meeting in a calendar appointment;
> - photograph information - such as the time/date and location it was taken; and
> - contact 'mailto' addresses within a webpage

It should be clear from the above that **the statement in the Draft Decision (presumably provided by the UK Government and accepted by the Commission) that "*Secondary data [once separated from the intercepted communication] would not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication*" is patently false**. It may to some extent be true in relation to *some* "systems data" (such as – tellingly – the ones given as examples) – but it certainly not true in relation to email addresses and user IDs, and of course not in relation to "identifying data" (as the very term makes clear).

On the contrary, under EU law email address and location data and other data linked to a person all constitute personal data – and it is now recognised by the European Courts that metadata ("secondary data" or "related communications data") can be as revealing and intrusive as, and in certain circumstances is even more revealing and intrusive than, communication content data. Thus (as already noted in our submission),[28] the European Court of Human Rights was:[29]

> **not persuaded that the acquisition of related communications data is necessarily less intrusive than the acquisition of content.** For example, the content of an electronic communication might be encrypted and, even if it were decrypted, might not reveal anything of note about the sender or recipient. The related communications data, on the other hand, could reveal the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted. In bulk, the degree of intrusion is magnified, since the patterns that will emerge could be capable of painting an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with.

The CJEU also stresses, if anything more strongly than the ECtHR, that communications data are highly revealing, can be used to create **profiles** of individuals, and are therefore "**no less sensitive than the actual content of communications**":[30]

---

[28] See Korff-Brown Submission to EU re UK adequacy, Part Two re UK surveillance (footnote 17, above), section 2.2.2, at iii (pp. 14 – 15).

[29] ECtHR First Section judgment in *Big Brother Watch [BBW] v. the United Kingdom*, 13 September 2018 (referred to the Gran Chamber on 4 February 2019 and still pending there), para. 356, emphasis added, available at:
https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-186048%22]}

[30] CJEU *Privacy International* Grand Chamber judgment of 6 October 2020, para. 71; *LQDN and Others* Grand Chamber judgment of the same date, para. 117.

> The interference with the right enshrined in Article 7 of the Charter entailed by the transmission of traffic data and location data to the security and intelligence agencies must be regarded as being particularly serious, **bearing in mind inter alia the sensitive nature of the information which that data may provide and, in particular, the possibility of establishing a profile of the persons concerned on the basis of that data, such information being no less sensitive than the actual content of communications.** In addition, it is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.

We therefore concluded that:[31]

The "Related communications data" that are extracted by the UK's GCHQ from the selected bearers indiscriminately, in bulk, and retained for some time, are highly revealing of the lives of the tens or hundreds of thousands of individuals to which they may relate, including EU persons (the vast majority of whom will have no links to terrorism or serious crime), can lead to them being profiled, and may have a chilling effect on their enjoyment of other rights such as the rights to freedom of communication, expression and association.

Recitals 223 and 233 and footnote 288 in the Draft Decision, quoted above, effectively seek to exclude the use of "secondary data" from scrutiny under the CJEU/EEG standards. But in fact, the use of metadata should be given special attention, for three related reasons.

First, as noted in the quotes from the European Court of Human Rights and the CJEU, above, rather than being innocuous, such data can be highly revealing, also of highly intimate and sensitive matters such as race, religion or sexual orientation. It should follow from this that indiscriminate collection of metadata should be regarded as compromising the very essence of the right to privacy (just as the CJEU held that indiscriminate collection of communication content compromises that essence).

Second, automated analyses of metadata are increasingly central to the UK (and the USA) intelligence activities. We have described them in our submission,[32] where we explain that these technologies are subject to serious limitations that can lead to serious errors: see our discussion of the three main problems with algorithmic "Subject of Interest"-detection in our submission.[33]

Yet third, crucially, we also found that under UK data protection law:

- metadata are not meaningfully protected against undue access and bulk collection by the UK intelligence agencies;[34]
- the situation in relation to oversight over complex selectors and search criteria is still unclear;[35] while

---

[31] Korff-Brown Submission to EU re UK adequacy, Part Two re UK surveillance (footnote 17, above), section 2.2.2, at iii (pp. 14 – 15).

[32] *Idem*, section 2.3, *How the data are used*. See in particular sub-section 2.3.3, at ii, *Identifying new threats and previously unknown persons "of interest" through more sophisticated data mining* (pp. 17 – 24).

[33] *Idem*, pp. 23 – 24.

[34] *Idem*, section 3.2, at 1 – 3, under the headings *Are metadata subject to UK data protection law protections?*, *Is the bulk collection of communications data, in particular metadata, based on "law"?*, *Does the law allow for general, indiscriminate access to personal data and for its collection/extraction in bulk?*, *and Is the law only used to counter genuine serious threats to national security?*.

[35] *Idem*, at 5, under the heading *Is there an effective, independent and impartial oversight system over all aspects and phases of the surveillance/bulk data collection?* The latest information, in the IPCO Annual Report 2019 (footnote 23, above) makes clear that although there were plans to increase oversight over the choice of

- oversight over the much more sophisticated data mining analyses appears to not have been addressed at all.[36]

We therefore concluded in that respect that:

[T]he situation relating to the processing of metadata ("secondary data") by the UK intelligence agencies clearly does not meet the EU standards as set out, in particular, in the CJEU LQDN judgment, referenced in this regard in the EEGs.

However, the Draft Decision, by relying on the misleading representations in the quoted recitals, simply ignores these crucial issues.

5. <u>Transfer of data obtained in bulk to other third countries (recitals 236 and 222)</u>:

According to the Draft Decision

> According to [S. 109 of the UK DPA201], personal data is not allowed to be transferred to a country or territory outside the United Kingdom or to an international organization, unless the transfer is necessary and proportionate for the purpose of the controller's statutory functions or for other purposes provided for in Section 2(2)(a) of the Security Services Act 1989 or Sections 2(2)(a) and 4(2)(a)of the Intelligence Services Act 1994 [i.e., for the Security Service the prevention or detection of serious crime or any criminal proceedings, for the Intelligence Service the interests of national security, the prevention or detection of serious crime, or any criminal proceedings, and for the GCHQ any criminal proceedings].
>
> Finally, the IPA 2016 sets out further safeguards in relation to transfers to a third country of material collected through targeted interception, targeted equipment interference, bulk interception, bulk acquisition of communications data and bulk equipment interference (so-called "overseas disclosures"). In particular, the authority issuing the warrant must ensure that arrangements are in force for securing that the third country receiving the data limits the number of persons who see the material, the extent of disclosure and the number of copies made of any material to the minimum necessary for the authorised purposes set out in the IPA 2016.
>
> (recitals 236 and 237, one footnote quoted below, other footnotes omitted. The words in square brackets are taken from footnote 426)

A footnote at the end explains that:

> The arrangements must include measures for securing that every copy made of any of that material is stored, for as long as it is retained, in a secure manner. The material obtained under a warrant and every copy made of any of that material must be destroyed as soon as there are no longer any relevant grounds for retaining it.
>
> (footnote 433)

---

selectors and search criteria (to meet criticism from the ECtHR), the exact format of this inspection was yet to be agreed: para. 10.28, with reference to the ECtHR *Big Brother Watch* judgment and other criticism.

[36] *Idem*. Note that, as the Director of GCHQ put it, "*AI capabilities will be at the heart of [GCHQ's] future ability to protect the UK.*" Foreword by Director of GCHQ to <u>Pioneering a New National Security – The Ethics of Artificial Intelligence</u>, 2020, available at:
https://www.gchq.gov.uk/artificial-intelligence/index.html
This report notes the ethical issues and risks but does not yet say how they will be addressed. The IPCO report (footnote 23, above) makes no reference to AI or algorithms and only one to "machine learning" – where it notes that its technical advisory panel provided a briefing on "Hashing and Machine Learning" (para. 17.9).

This is also stressed elsewhere:

> Similar to what is provided for targeted interception, Part 6 of the IPA 2016 provides that the Secretary of State must ensure that arrangements are in force to provide safeguards on the retention and disclosure of material obtained under [a bulk interception or bulk equipment interference warrant], as well as for overseas disclosure. In particular, Sections 150(5) and 191(5) of the IPA 2016 require that every copy made of any of that material collected under the warrant must be stored in a secure manner and is destroyed as soon as there are no longer any relevant grounds for retaining it, while Sections 150(2) and 191(2) require that the number of persons to whom the material is disclosed and the extent to which any material is disclosed, made available or copied must be limited to the minimum that is necessary for the statutory purposes. Finally, when the material that has been intercepted either through a bulk interception or a bulk equipment interference is to be handed over to a third country ("overseas disclosures"), the IPA 2016 provides that the Secretary of State must ensure that appropriate arrangements are in place to ensure that similar safeguards on security, retention and disclosure exist in that third country.
>
> (recital 222)

What should be noted is that these conditions are very limited and almost entirely and solely concerned with data security. Personal data including bulk data (or data created from analysis of bulk data) can be disclosed by the UK intelligence agencies to the intelligence agencies of other third countries when the UK agencies believe this is necessary and proportionate for the purpose of the UK agency's statutory functions – i.e., broadly speaking, for national security purposes or in relation to serious crime – provided only that the recipient agency in the other third country treats the data securely.

The issue is apparently under review. The 2019 IPCO report says:

> **Sharing bulk data: Review of procedures at GCHQ**
>
> In our 2018 report, we explained that, in *Privacy International v GCHQ & Others IPT/15/110/CH*, the investigatory Powers Tribunal (IPT) had considered the lawfulness of GCHQ's use of certain bulk data. The IPT judgment, published on 23 July 2018, called for "*a review of existing procedures at GCHQ in relation to sharing of intelligence and of bulk datasets… under the supervision of IPCO*". In response, GCHQ conducted a detailed review of the processes and procedures governing decisions to share data in bulk with foreign partners and then implemented measures to bring about improvements. **In the future, this area will be covered as part of our regular oversight and inspection arrangements.**
>
> One significant challenge the review faced was the commencement, in August 2018, of the parts of the IPA relating to the various bulk powers. This included the implementation of the safeguards contained in the Act, the accompanying Codes and the involvement of JCs undertaking the double-lock of bulk warrants. This includes the requirement under the IPA that, **before approving the sharing of material obtained as a consequence of conduct under a bulk warrant, the Secretary of State must be satisfied *(to such an extent (if any) as the Secretary of State considers appropriate)* that the overseas authority with whom material is being shared has in place safeguards in relation to retention, disclosure and examination. In our supervisory role, we considered the adequacy of GCHQ's assurances to meet this requirement.**
>
> (paras. 10.41 – 10.42, emphases added)

This confirms that data sharing remains essentially an entirely discretionary matter in the hands of the Secretary of State, with a focus only on security and absolutely minimal judicial oversight (if any at all).

In our submission, we have shown that in fact the UK's GCHQ and the US's NSA operate much of the bulk surveillance programmes jointly – and share effectively all data (and analyses) so collected, and most of it also with the other "5EYES" countries, Australia, Canada and New Zealand:[37]

> **[The "5EYES" arrangement was established] for the purpose of sharing intelligence but primarily signals intelligence** derived from the interception of communications travelling and transmitted by fibre optic cables, radio waves, satellites, and other forms of wireless telegraphy.
>
> … **from the outset, the relationship was a highly integrated one, particularly as it concerned the cooperation of American and British agencies.**
>
> [I]n addition to facilitating collaboration, the [UKUSA] agreement suggests that **all intelligence material is shared between Five Eyes States by default**. (para. 76)
>
> [The "5EYES" arrangement … **relies on [the agencies] shar[ing] the collection burden and the resulting intelligence yield**.
>
> **The level of co-operation under the UKUSA agreement is so complete that "*the national product is often indistinguishable.*"**

We concluded that:

[T]he extensive – indeed, it would appear, comprehensive – data sharing arrangement between the "5EYES" agencies, and more in particular between GCHQ and the NSA, means that data on individuals in the EU, and in particular their communications data, collected in bulk by GCHQ, will (continue to) be made available also to the NSA – and indeed analysed in the manner described earlier jointly by GCHQ and NSA staff.

In terms of the GDPR, this sharing will, at least from 1 January 2021, involve the "onward transfer" of the data on individuals in the EU from the UK to the USA.

While the UK was an EU Member State, perhaps not much could be done about this under EU law. However, now that the UK is no longer an EU Member State this can, and we submit must, be addressed urgently, in general and in the context of the matter of a UK adequacy decision.

There is nothing to indicate that this has in any way changed because of the review mentioned in the ICPO report. But once again, the Draft Decision effectively ignores this crucial issue.

- o – O – o –

[37] The quoted are from the witness statement of Privacy International's then deputy director, Eric King, to the Investigatory Powers Tribunal in the case brought by PI against the agencies. Fuller quotes, with references to King's testimony where full references are given for all his evidence, are provided in Part Two of our submission (footnote 17, above), in section 2.4, *The UK-USA (and wider "5EYES") collaboration*.

III. Monitoring of the adequacy decision

As the Commission notes in the Draft Decision, under Article 45(4) GDPR it is required to "monitor developments in third countries" that have been granted a positive adequacy decision under the GDPR or under the 1995 Data Protection Directive, and it must do so "on an ongoing basis".

The Draft Decision stresses this monitoring by the Commission specifically in relation to the still to be clarified details of the UK-US Agreement discussed at 3.3, above (recitals 153 – 154), but also generally (section 6, *Monitoring, suspension, repeal or amendment of this decision*) because:

> Such monitoring is particularly important in this case, as the United Kingdom will administer, apply and enforce a new data protection regime no longer subject to European Union law and which may be liable to evolve.
>
> (recital 274)

In accordance with Article 45(5), the Draft Decision notes that if "available information" were to show that the UK no longer provided adequate protection, the Commission may repeal, amend or suspend the decision (recital 278). "On duly justified imperative grounds of urgency", the Commission can even do make such repeal, suspension or amendment "immediately applicable" (recital 280). But normally, if the Commission were to have doubts as to the UK's continued adequacy, it would first notify the UK of this and "request that appropriate measures be taken within a specified, reasonable timeframe" (recital 277).

To facilitate this monitoring:

> the United Kingdom authorities are invited to inform the Commission of any material change to the UK legal order that has an impact on the legal framework that is the object of this Decision, as well as any evolution in practices related to the processing of the personal data assessed in this Decision.
>
> Moreover, in order to allow the Commission to effectively carry out its monitoring function, the Member States should inform the Commission about any relevant action undertaken by the national data protection authorities, in particular regarding queries or complaints by EU data subjects concerning the transfer of personal data from the Union to controllers or processors in the UK. The Commission should also be informed about any indications that the actions of United Kingdom public authorities responsible for the prevention, investigation, detection or prosecution of criminal offences, or for national security including any oversight bodies, do not ensure the required level of protection.
>
> (recitals 275 – 276)

Stipulation on the above lines can be found in all adequacy decisions including all those taken under the 1995 Data Protection Directive and the single one adopted so far under the GDPR (on Japan).

However, the Commission has **never** repealed, suspended or amended any adequacy decision even when it would be clear from even a cursory examination of a country's law and practices that (whatever the original situation when assessed under the 1995 Directive) the country does not provide for adequate protection in terms of the GDPR, as clarified by the CJEU in *Schrems I* ("essentially equivalent").

The situation in relation to **Israel** is illuminating in this regard. The 2011 adequacy decision on the country was adopted under much less demanding standards set out in a very early WP29 document (WP12 of 24 July 1998), that allowed for the issuing of a positive adequacy decision if the rules in the country concerned were roughly similar to those in the then applicable Data Protection Directive – or even, if the Commission believed that the third country was in the process of moving closer to the EU rules (*in casu*, the WP29 and the Commission expressly relied on proposals in the Schoffman Report that had then just been published – but those proposals were never implemented). In fact, the 1981 Israeli Privacy Protection Act has hardly changed since 2011 and is manifestly not adequate in terms of – and very far from "essentially equivalent" to – the GDPR. For instance, the list of sensitive data does not include the categories of ethnic origin or sexual preferences. Consent can be implied. There is very extensive surveillance by the Israeli defence and intelligence agencies under rules that clearly do not meet the CJEU standards as reflected in the EDPB's European Essential Guarantees for surveillance. The supervisory authority is not fully independent of the executive. And the stipulations on the territorial scope of the adequacy decision and on onward transfers of personal data are simply not complied with. Yet the 2011 adequacy decision on Israel is still in place (it is now supposed to be under review because the GDPR requires such a review – and it is difficult to see how it can be maintained, but the Commission has not yet given any indication of what action, if any, it intends to take).

Similar issues arise in relation to other third countries that have been granted adequacy decisions over the years.

In the circumstances, not too much should be expected of the "ongoing monitoring" by the Commission of the situation in the UK after the UK decision comes into force (if it ever does).

- o – O – o -

Douwe Korff (Prof.
Cambridge, UK, 3 March 2021