Professor Elaine Fahey, Professor of Law and Humanities, City, University of London and Dr Elif Mendos Kuşkonmaz, Lecturer in Law, University of Essex – Written Evidence (DAT0011)

The House of Lords European Affairs Committee – Data Adequacy Inquiry
Written Evidence submitted by Professor Elaine Fahey, Professor of Law and Humanities, City, University of London and Dr Elif Mendos Kuşkonmaz, Lecturer in Law, University of Essex

The following submission represents the views of Professor Elaine Fahey (Professor of Law and Humanities) from City, University of London and Dr Elif Mendos Kuşkonmaz (Lecturer in Law) from the University of Essex. Professor Fahey is an expert in the areas of EU law, global governance, trade, transatlantic relations, the EU's Area of Freedom, Security and Justice. Dr Kuşkonmaz is an expert in privacy and data protection, data access and transfer regimes, state surveillance and human rights.

2. What are the possible challenges to the UK-EU data adequacy regime?

a. What factors could influence the next European Commission when deciding whether to renew its data adequacy decisions for the UK in June 2025?

Several factors could influence the European Commission's decision to renew the UK's adequacy status. The crucial factors are respect for human rights, national security law, criminal law, public authorities' access to data, onward data transfers to third countries, effective independent supervisory authorities, and international commitments under binding treaties and conventions.[1] These factors played a significant part in the Commission's initial assessment. They will continue to feature in determining whether the UK affords an adequate level of protection to individuals for processing their data, mainly in case of a legal challenge.

b. What factors could the Court of Justice of the EU (CJEU) consider if the legality of the EU-UK adequacy decisions were challenged?

The abovementioned factors raise potential avenues for challenging the EU-UK adequacy decisions before the CJEU.[2] The UK surveillance law

[1] Art 45(2), General Data Protection Regulation; Art 36(2), Law Enforcement Directive.
[2] C-362/14 *Maximillian Schrems v Data Protection Commissioner* ECLI:EU:C:2015:650 ('*Schrems I*'); Opinion 1/15 [2016] ECLI:EU:C:2016:656; C-311/18 *Data Protection Commissioner v Facebook Ireland and*

was a central point of contention as the European Commission deliberated its initial assessment of the UK's adequacy status. The compatibility of the UK surveillance law with the fundamental rights standards the CJEU seeks in a third country will continue to be a live issue in case of a legal challenge. The CJEU already considered the UK law on data retention and access regime incompatible with the EU fundamental rights standards in *Privacy International,* which concerned the regime preceding the Investigatory Powers Act (IPA) 2016.[3] This decision and similar decisions by the CJEU show that the Court does not give unwavering support for general data retention regimes. If the UK's adequacy status were to be challenged, the Court could consider the nature of the national security deficit requiring a general data retention regime (i.e., there must be a serious threat to national security, and that threat must be genuine and present or foreseeable) and the powers of the independent body reviewing why general data retention measure is authorised. [4] The CJEU could then scrutinise the double lock system introduced in the IPA 2016 and the exclusive jurisdiction of the Investigatory Powers Tribunal (IPT) over the claims relating to the surveillance powers under the IPA 2016.

There is a risk that the Judicial Commissioner's power to review the bulk data retention authorisation does not match what the CJEU requires from the review bodies because his review power is limited to considering the necessity and proportionality of the issued warrant based on the operational purposes stated therein and he does not have the power to review the nature of those purposes independently. The IPT could be a satisfactory safeguard given that the ECtHR upheld its ex-post supervisory power[5], but its findings will be the *minimum* benchmark for the CJEU's scrutiny of the UK data protection regime.[6] The CJEU could further consider the extent to which the IPT has the powers it seeks from an effective and independent review authority.

The existence of an independent review body with efficient powers is not the only area where the CJEU might call the UK adequacy status in question. How the IPA 2016 prescribes certain surveillance powers for the executive would come under the CJEU's scrutiny. Whether the relevant rules satisfy the clarity and precision that the CJEU requires from the legally prescribed surveillance powers is questionable.[7] The CJEU seeks the law to limit the surveillance powers with specific criteria instead of

---

Maximillian Schrems ECLI:EU:C:2020:559 ('*Schrems II'*).

[3] C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* ECLI:EU:C:2020:790 ('*Privacy International'*).

[4] Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v Premier Ministre and Others* ECLI:EU:C:2020:791 ('*La Quadrature du Net*'), para 168.

[5] *Kennedy v the UK* (2011) 52 EHRR 4; *Big Brother Watch and others v UK* Appl nos 58170/13, 62322/14, and 24960/15 (25.05.2021).

[6] Valsamis Mitsilegas et al., 'Data Retention and the Future of Large-Scale Surveillance: The Evolution and Contestation from the Benchmarks' (2022) European Law Journal, available at <https://onlinelibrary.wiley.com/doi/10.1111/eulj.12417> accessed 1 May 2024.

[7] *Schrems II*, para 176; *La Quadrature du Net*, para 132.

requiring that authorities' access to the data be consistent with the objective pursued by that law.[8] The IPA 2016 is, however, more enabling than the CJEU permits. The necessity and proportionality requirements and several factors included in the Act work as the standards for the Secretary of State to perform the discretionary power. This is different from having legally prescribed concrete conditions to issue a warrant. These two exemplary points show that the IPA 2016 could be subject to the CJEU's strict scrutiny. The proposed amendments under the Investigatory Powers Act (Amendment) Bill could compound the compelling legal issues around the IPA 2016 because several clauses might undermine the protection offered to the EU-originated data. This would ultimately frustrate the UK's adequacy status before the CJEU.

If the adequacy framework is challenged, the CJEU will also consider the onward data transfer regime under UK law. The UK-US CLOUD Agreement could be another issue risking the longevity of this framework. US authorities can access the EU-originated data through the UK-US CLOUD Agreement after they are lawfully transferred to the UK under the EU-UK adequacy decisions. The US adequacy status has been contentious since the CJEU's *Schrems* decisions, and this issue has still not been settled for the EU. This means that the UK-US CLOUD Agreement could be a potential roadblock for the UK to maintain its adequacy status, mainly where the third EU-US adequacy decision follows the fate of its predecessors. Equally, any future data-sharing arrangement similar to the UK-US CLOUD Agreement that the UK signs with a third country can be strictly scrutinised by the CJEU. The contents of any such arrangements must be considered diligently to ensure that they do not water down the protection offered to data subjects and the EU-originated data under UK law.

Finally, the ongoing discussions around repealing the Human Rights Act 1998 or withdrawing from the ECHR, which would weaken human rights protection, can imperil the maintenance of adequacy status. The UK's continuing adherence to the ECHR is even more critical for its data protection regime now that national law does not recognise personal data protection as a fundamental right.[9] Any potential weakening of privacy rights protection under the ECHR will threaten the UK's adequacy status.

c. How would you assess the possible impact of proposed UK rules on automated decision-making and the use of Artificial Intelligence on data adequacy?

The UK Government is adamant about relaxing the regulation of automated decision-making to support innovation, but the amendments to the existing rules can raise issues for the CJEU to uphold the UK's adequacy status. Currently, the UK GDPR gives individuals the right not to

[8] *La Quadrature du Net,* para 176; *Privacy International*, para 77.
[9] Data Protection (Fundamental Rights and Freedoms) Regulations 2023/1417.

be subjected to solely automated decisions. This right is subject to limited exceptions, all of which must exhibit suitable measures and safeguards for the fundamental rights protection of individuals. The proposed rule on automated decision-making adopts a more permissive language to the detriment of fundamental rights protection by giving prior acceptance to the data controller to conduct automated decision-making. This is a complete removal of the individual right against automated decision-making in the first place.

Also, the proposed rules contradict the prohibition against automated decision-making prescribed under the Council of Europe's Convention 108+. The Convention overlaps closely with the prohibition in the General Data Protection Regulation (GDPR) and, ultimately, in the UK GDPR.[10] Even though the supremacy of the GDPR as the retained EU law ceases to exist[11], the CJEU could call the UK's existing international commitment under Convention 108+ into question. The divergence from the current rule on automated decision-making would undermine the protection afforded to individuals. It might lead the CJEU to consider that the UK does not adhere to internationally binding treaties, and its legal framework undermines the data protection afforded to individuals. This might ultimately raise an issue for the UK's adequacy status.

3. What implications, if any, would a no or disrupted UK-EU data adequacy scenario have?

a. Do you have any concerns about the direction of travel of the UK Government's data policies as set out in the Data Protection and Digital Information Bill, and about the potential for greater divergence from EU data standards?

Even though there is no expectation under EU international data transfer rules that UK law should mirror the EU data protection regime, the European Commission paid particular attention to the UK's close alignment with the EU data protection acquis in granting the UK an adequacy status. In this context, the UK occupies a more peculiar position than other third countries as a former EU Member State whose national law had been amended according to the obligations under EU law harmonisation initiatives. Divergence from the existing data protection legislation that negatively affects the protection afforded to personal data and data subjects would imperil the UK's adequacy status.

The prevailing government policy of complex managed divergence is difficult to understand, given its multifarious directions and lack of certainty. Key EU developments with important international partners such as the US and the EU-US Data Privacy Framework Agreement with an independent court suggest that the UK direction of travel could be vulnerable to challenge at national, regional and international levels,

[10] Art 9, Convention 108+.
[11] The Retained EU Law (Revocation and Reform) Act 2023.

exposing divergences that cumulatively undermine the adequacy framework itself.

b. How high is the risk of the European Commission withdrawing its UK data adequacy decisions? What impact would that have and how prepared are businesses or the public sector for such a scenario?

The risk of withdrawing the adequacy decision must be deemed to be moderate in the current legal framework prevailing in the absence of any legal action. However, sustained critique of the UK's emerging and existing legislation infrastructure to which the decision relates must be engaged with where possible.

c. What would be the implications for the continued operation of Part III of the TCA (law enforcement and judicial cooperation on criminal matters)?

Part III of the TCA must be read alongside the Commission's existing UK adequacy decisions to understand the rules on information sharing for law enforcement purposes. This Part provides more detailed data processing and sharing rules for specific information-sharing schemes such as Passenger Name Records (PNR), Prüm, and the European Criminal Records Information System (ECRIS). However, certain aspects must be reconsidered to sustain an adequate level of protection for individuals. For example, the CJEU laid out further fundamental rights standards for PNR data processing. This means that some of the provisions of Part III of the TCA are vulnerable to future legal challenges based on the CJEU's deliberations on the PNR processing.[12] Several pending preliminary ruling requests on the same issue will allow the Court to reiterate and expand on its observations. Part III of the TCA and its provisions on law enforcement information sharing must be reconsidered for their observance of the emerging fundamental rights standards to which the UK will be held.

4. What can be learned from other countries' experience with the adequacy system and engagement with the European Commission's process?

a. What conclusions do you draw from the European Commission's recent adequacy review of 11 countries and territories?

The European Commission has adopted a heavily 'Executive-dominant' approach to developing adequacy decisions. The Report on the first review of the functioning of the adequacy decisions adopted pursuant to

[12] Elaine Fahey, Elspeth Guild, and Elif Mendos Kuşkonmaz, 'The Novelty of EU Passenger Name Records (PNR) in EU Trade Agreements: On Shifting Uses of Data Governance in Light of the EU-UK Trade and Cooperation Agreement' (2023) 8(1) European Papers 273, <https://www.europeanpapers.eu/en/e-journal/novelty-eu-passenger-name-records-eu-trade-agreements> accessed 1 May 2024.

Article 25(6) of Directive 95/46/EC is not a particularly critical or onerous set of reviews. The CJEU has 'inserted' itself into the process in a fashion that has proven to be disruptive but has not per se been successful in altering the direction of the rollout of adequacy decisions, as is exemplified by the review process. Key shifts in partner practices regarding data transfers, e.g. as to COVID-19, e.g. as to Israel and important nuances in digital trade chapters with partners, e.g. Japan, have not operated adversely as to the adequacy review process. It remains to be seen whether these broader trends can continue. The European Parliament's opposition to the UK adequacy decision on civil liberties grounds is echoed as to the EU-UK adequacy decision, and litigation cannot be ruled out going forward.

b. Are there examples of best practice which the UK could learn from in the way other countries approach their data transfer arrangements with the EU?

To a degree, the UK will always be held to a different standard implicitly on account of its historical background. EU-Japan arrangements have many consequences, as the first post-GDPR data flow agreement resulted in an adequacy decision. Recently, the EU and Japan have agreed on a soft law digital partnership, and the EU-Japan Digital Trade chapter data flow provisions have not operated with the esoteric nuance anticipated.[13] It would appear difficult to emulate the example of the EU-US Data Privacy Framework Agreement, with an independent court part thereof, evolved as a response to the infamous *Schrems* litigation before the CJEU.[14]

c. What are the implications for the UK's EU adequacy status if the UK grants its own adequacy decisions to other third countries currently not subject to EU adequacy?

The European Commission and the CJEU consider onward transfers of EU-originated data when determining the UK adequacy framework. The UK GDPR echoes the list of factors included in the EU data protection law, but there is a risk that the CJEU might not be satisfied with the extent of the adequacy review conducted by the Secretary of State if it considers that the onward transfers circumvent the EU data transfer rules and thus watering down the protection offered to the EU-originated data by UK law. A more urgent point is the direction the UK Government wants to take with the UK international data transfer rules under the Data and Digital

[13] Elaine Fahey and Isabella Mancini 'Cross-border data flows between the EU, UK and Japan' (2023) 49 *Keio Law Journal* 61, available at <https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/download.php/AA1203413X-20230330-0061.pdf?file_id=174438> accessed 1 May 2024.

[14] Elaine Fahey ad Fabien Terpan, 'The Future of the EU-US Privacy Shield' 221-236 in Elaine Fahey (Ed.) *The Routledge Research Handbook of Transatlantic Relations* (Routledge 2023); Elaine Fahey and Fabien Terpan, 'Torn Between Institutionalisation & Judicialisation: The Demise of the EU-US Privacy Shield' (2021) 28(2) *Indiana Journal of Global Legal Studies* 205, available at <https://www.repository.law.indiana.edu/ijgls/vol28/iss2/5> accessed 1 May 2024 .

Information Bill. The proposed rules diverge greatly from the existing rules around adequacy requirements with the phrasing of allowing data transfer to countries whose legal order is not 'materially lower' than the protection provided under the UK data protection regime. It is unclear what this materially lower standard is. If this standard is lower than the adequacy standard required under the EU, the EU-UK adequacy decision will be more vulnerable to a legal challenge.

d. If the UK joined the Global Cross Border Privacy Rules system, what impact if any could that have on the UK's EU adequacy status?

Other international standards, such as APEC CBPR, could become geographically more significant in the advent of broader membership, particularly from larger jurisdictions, such as the UK post-Brexit. However, the EU might join the CPTPP to thwart the UK's intentions, but it might also alter this complex dynamic as to the EU's place. The CBPR is adopted in many jurisdictions that are notably increasingly adopting privacy frameworks. It is arguably at variance with the travel direction, i.e., regulating data flows using binding hard law and adopting privacy standards. Moreover, the G7 digital trade provisions have been agreed to have data-free flows with trust, and a Global Digital Compact is under agreement at the UN level, particularly with European influence.

There are still highly divergent views on the place of privacy and data rights in US legal order, despite the EU-US Trade and Technology (TTC) and EU-US Data Privacy Framework Agreement. The US was publicly relaunching CBPR as a global privacy standard to rival the EU's GDPR, perhaps oddly given the depth of convergence allegedly at the heart of the EU-US Data Privacy Agreement, but this appears less politically prominent in recent times.[15] The development also risked conflict with APEC CBPR, which appears still to be under development. Thus, further divergence may still occur, but it could also place the UK in a vulnerable position through its multiparty relations. The Global CBPR still appears to be heavily trade-related.

It would be a highly dramatic development for the UK to join an opposing world global regime that is the only standard of many Asian countries not noted for their capacity to support strong rights-based regimes. Given the number of countries joining the GDPR it seems

[15] Anupam Chander, 'Is Data Localization a Solution for Schrems II?' (2020) 23 *Journal of International Economic Law* 771; Paul Schwartz, 'The EU-US Privacy Collision: A Turn to Institutions and Procedure' (2013) 126 Harvard Law Review 1996; Cf. Svetlana Yakovleva and Kristina Irion, 'Pitching trade against privacy: reconciling EU governance of personal data flows with external' (2020) 10(3) *International Data Privacy Law* 201; Asia-Pacific Economic Cooperation (APEC), *Cross Border Privacy Rules (CBPR)*, available at <http://cbprs.org/> accessed 1 May 2024; Anupam Chander and Paul Schwartz "Privacy and/or Trade," (2023) 90(1) *University of Chicago Law Review* 49, available at <https://chicagounbound.uchicago.edu/uclrev/vol90/iss1/2> accessed 1 May 2024.

somewhat counterintuitive to sign up to systems at variance with those in-situ.

Received 3 May 2024