Data transfers between the EU and UK post Brexit?

DATA TRANSFERS BETWEEN THE EU AND UK POST BREXIT?

Andrew D. Murray, Law Department, LSE

Original Article

Summary

- Changes to the UK constitutional and institutional settlement on Brexit day may affect the likelihood of the UK securing an adequacy decision under GDPR.
- Despite the UK Government claiming that on Brexit day, "it will have fully implemented EU [data] privacy rules" it will have no equivalent of Article 8 of the EU Charter in domestic law.
- This may undermine efforts to achieve an adequacy ruling due to the decision of the CJEU in *Maximillian Schrems v Data Protection Commissioner.*
- The UK's decision to continue with a data retention regime in Part 4 of the Investigatory Powers Act 2016 could also be at odds with the Article 8, Charter right.
- Conflict between the domestic legal settlement of the Investigatory Powers Act 2016 and the decision of the CJEU in *Tele2 Sverige AB v Post-och telestyrelsen* may also imperil an adequacy decision.

Keywords: Adequacy, Brexit, Data Retention, EU Charter, GDPR, UK Law.

I: INTRODUCTION: THE UK GOVERNMENT'S POSITION

On 1 February 2017, Matt Hancock, Minister of State for Digital and Culture, and part of the UK Government team responsible for policy in relation to data protection, as well as implementation of the GDPR, appeared before the EU Home Affairs Sub-Committee. The Committee were keen to hear from the Minister the Government's plans to ensure the continued flow of data from the European Union to the UK after Brexit. Confirming that the UK Government

intended to implement the GDPR fully, and that they would not seek to make any significant changes to UK data protection law post Brexit, he noted that the Government was "keen to secure the unhindered flow of data between the UK and the EU post-Brexit and we think that signing up to the GDPR data protection rules is an important part of helping to deliver that".[1] While the Minister was keen to stress the UK Government would seek to ensure the unhindered exchange of data within an appropriate data protection environment he would not be drawn on whether the UK Government believed an adequacy decision would be necessary before "Brexit Day" on 29 March 2019 (assuming no extensions to negotiations) and refused to be drawn on the processes while negotiations were on-going. When directly asked the question "If you do not secure an adequacy decision what is the default position?" the Minister responded rather blandly "we are seeking unhindered data flows, and that we are confident we will achieve."[2]

In a later appearance before the same Sub-Committee, Baroness Williams, Minister of State at the Home Office placed on the record "the importance that the Government places on Data Protection and [their] commitment to ensuring robust safeguards are in place."[3] She argued that "the U.K. will enjoy a unique position as a third country seeking data transfers with the EU, given that, unlike

[1] The Rt. Hon Matt Hancock, evidence to the EU Home Affairs Sub-Committee, 1 February 2017: http://www.parliamentlive.tv/Event/Index/b3334d4c-93bf-4aca-9df5-666b7a72c06c (at 10:49:32 - 10:49:53).
[2] Ibid, 11:02:35 – 11:03:03.
[3] Baroness Williams of Trafford, evidence to the EU Home Affairs Sub-Committee, 26 April 2017: http://parliamentlive.tv/Event/Index/ed6b1fe1-c786-4768-9e63-a65b994cc8d7 (at: 11:02:50 - 11:03:07)

other non-EU countries, it will have fully implemented EU [data] privacy rules."[4] Like her colleague Mr Hancock though she refused to be drawn on the details of any post-Brexit settlement.

It is clear therefore that the position of the UK Government is that the UK will continue to trade data with EU27 states following Brexit and that this should be "unhindered". It also appears to be the view of the Government that to achieve a settlement to allow this to happen will be quite uncontentious given that in the words of Baroness Williams, "obviously on the day that we leave our laws are compatible with those of the EU",[5] however this paper will argue that this is not as clear-cut as Government Ministers seem to be assuming. The morning we leave the European Union a number of institutional and constitutional differences will be in place. Baroness Janke, in a question to Mr. Hancock, alluded to at least one of those differences: "If we will no longer be under the Jurisdiction of the European Court of Justice, how do you anticipate who will be the [] final adjudicator in such matters?"[6] This is a significant question given Recital 41 of the GDPR:

> [w]here this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, ***in accordance***

[4] Ibid, 11:08:17 – 11:08:24.
[5] Ibid, 11:10:29 – 11:10:36.
[6] Above n.1, 10:40:30 – 10:40:58.

with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights.[7]

The significance of Recital 41 should not be under-estimated for reasons we shall see below. The response from Mr. Hancock was in light of this less than encouraging: "there are several different ways that that can take place but [] we don't have the answer to that question."[8]

II: BREXIT AND THE FUNDAMENTAL RIGHT TO DATA PROTECTION

Brexit will have legal implications far beyond the sphere of data protection and while data protection and data transference may be described as a "high priority" by Minsters[9] it must compete for attention alongside other "high priorities" such as immigration controls; a common travel area with Ireland; investment in science and innovation; and a common approach to fighting crime and terrorism. All of these were listed as being among the government's twelve priorities for Brexit in the Prime Minister's speech of 17 January 2017, which pointedly did not list data protection and data transference among her priorities.[10] This may explain the apparent approach of the Government: to serendipitously continue to apply in domestic law the GDPR and related Directives that will have come into effect on or by 25 May 2018 in full; to ensure in their words "an uninterrupted and unhindered" flow of data between the UK

[7] Emphasis added.
[8] Above n.1, 10:40:58 – 10:41:06.
[9] Statement of Matt Hancock to the House of Lords European Union Committee as recorded at para.143 in Brexit: the EU data protection package, 3rd Report of Session 2017–18. Available from: https://publications.parliament.uk/pa/ld201719/ldselect/ldeucom/7/7.pdf.
[10] The Rt. Hon Theresa May MP, *The government's negotiating objectives for exiting the EU*, 17 January 2017. Available from: https://www.gov.uk/government/speeches/the-governments-negotiating-objectives-for-exiting-the-eu-pm-speech.

and EU27 post Brexit. However, as Baroness Janke explored, much of the constitutional and institutional landscape will be very different on 29 March 2019. The EU institutions will be outwith the UK's legal and constitutional framework and thus institutions such as the Commission and the Court of Justice will have no direct authority. The UK will also no longer be a member of the new European Data Protection Board (EDPB), for the Board is "composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives."[11]

The EDPB is considerably more powerful than the Article 29 Working Party with expanded roles and influence. The EDPB shall be an EU body[12] and will have specific legal authority to act independently.[13] The EDPB will be tasked with ensuring consistency of GDPR application throughout the EU and will issue guidelines and opinions to supervisory authorities when certain measures are adopted.[14] A key role of the EDPB will be to issue binding decisions where conflicts arise between supervisory authorities, giving the EDPB a quasi-judicial function.[15] Further, and crucially for the UK, the EDPB under is tasked with "provid[ing] the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country, including for the assessment whether a third country, a territory or one or more specified sectors within that third country, or an international organisation no longer ensures an adequate level of

[11] Regulation (EU) 2016/679 of the European Parliament of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Art.68(3), OJ 2016 L 119/1.
[12] Ibid, Art.68(1).
[13] Ibid, Art.69(1).
[14] Ibid, Arts.64 & 70.
[15] Ibid, Art.65.

protection."[16] Thus the EDPB will advise the Commission of the UK's adequacy under the GDPR but more importantly will continue to monitor the UK's compliance. This suggests that should the UK fail to accept any decision of the EDPB; it may lose its adequacy status. This means the UK will have to accept decisions of the EDPB without representation on the Board, a position likely to be quite unpalatable to those who view Brexit as a complete divorce from EU institutions.

The UK's rights framework will also change for, as the UK Government White Paper on the Great Repeal Bill states:

> The Charter (of Fundamental Rights) only applies to member states when acting within the scope of EU law, so its relevance is removed by our withdrawal from the EU…It cannot be right that the Charter could be used to bring challenges against the Government, or for UK legislation after our withdrawal to be struck down on the basis of the Charter. On that basis ***the Charter will not be converted into UK law by the Great Repeal Bill***."[17]

The White Paper suggests that withdrawal from the EU Charter will cause no change to the established rights framework of the UK:

> The Government's intention is that the removal of the Charter from UK law ***will not affect the substantive rights that individuals already benefit from in the UK***. Many of these underlying rights exist elsewhere in the body of EU law which we will be converting into UK law. Others

[16] Ibid, Art.70(1)(s).
[17] Department for Exiting the European Union, *Legislating for the United Kingdom's withdrawal from the European Union*, Cm 9446, March 2017: [2.23] (emphasis added).

> already exist in UK law, or in international agreements to which the UK is a party. As EU law is converted into UK law by the Great Repeal Bill, it will continue to be interpreted by UK courts in a way that is consistent with those underlying rights. Insofar as cases have been decided by reference to those underlying rights, that case law will continue to be relevant. In addition, insofar as such cases refer to the Charter, that element will have to be read as referring only to the underlying rights, rather than to the Charter itself.[18]

One specific right, which is not to be found in UK law, or in other international agreements, is Article 8 of the EU Charter:[19] the Data Protection Right. Clearly the UK Government will point to their intention to implement the GDPR as evidence that data protection rights are included in that body of "underlying rights [which] exist elsewhere in the body of EU law which we will be converting into UK law."[20] However it may be argued that there is a difference between the fundamental right to data protection found in the Article 8, and the provisions of the GDPR which provides a framework for the recognition and enforcement of the fundamental right. This right/framework distinction is acknowledged within the GDPR at Article 1(2) where it acknowledges "[t]his Regulation ***protects*** fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data." The distinction between the roles of the Charter right and the GDPR is fine but important. The Charter (which holds

[18] Ibid, [2.25] (emphasis added).
[19] Charter of Fundamental Rights of the European Union 2000/C 364/01, OJ 2012 C 326/391.
[20] See also Cl.3(1) of the European Union (Withdrawal) Bill 2017-19: 'Direct EU legislation, so far as operative immediately before exit day, forms part of domestic law on and after exit day.'

treaty equivalence)[21] affords the right to data protection; the GDPR, which does not have treaty equivalence, is the framework to ensure this right is recognised and protected. Therefore it can clearly be argued that when the UK leaves the EU, and thereby the EU Charter, UK citizens (and EU citizens looking to enforce in the UK) will lose their ***right*** to data protection as found in Article 8 of the Charter. They will retain only the shadow of the right through the framework for data protection which will be found in the UK implementation of the GDPR. This essential distinction has a number of immediate implications. A domestic UK Data Protection Act cannot adequately replace the fundamental right to data protection found in the EU Charter. Such an Act, which is always subject to Parliamentary repeal, will only replicate the framework of data protection as found in the subordinate EU Legislation (the GDPR). Only if the UK Government were to adopt a right to data protection in some form in the proposed British Bill of Rights would there be true equivalence for Article 8 in domestic law. It may be argued that other UK international obligations such as Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its additional protocol[22] or the OECD Privacy Framework[23] could substitute for Article 8, but importantly for this analysis these international legal instruments do not hold the same constitutional status as the EU Charter both requiring domestic implementation.

[21] Art.6(1), Treaty on European Union 2012/C 326/01, OJ 2012 C 326/3.
[22] CETS 108, 28 January 1981 and ETS 181 8 November 2001.
[23] http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

This all becomes important when rights are thrown into conflict and domestic UK courts will become the final arbiter of data protection law in the UK.[24] As Advocate General Jääskinen demonstrated in *Google Spain SL and another v Agencia Española de Protección de Datos and another*,[25] there is a clear legal distinction between the Charter Right and the Directive (or Regulation) which gives effect to them.

> According to the ECHR and the Charter any interference to protected rights must be based on law and be necessary in a democratic society. In the present case we are not faced with interference by public authorities in need of justification but of the question of the extent that interference by private subjects can be tolerated. The limits to this are set out in the Directive, and they are thus based on law, as required by the ECHR and the Charter. ***Hence, when the Directive is interpreted, the exercise precisely concerns the interpretation of the limits set to data processing by private subjects in light of the Charter.***[26]

As will be argued below, this matters. There will no longer be a fundamental right to data protection in the UK post Brexit and this is something which cannot be remedied through domestic legal settlements short of a British Bill of Rights, and even then perhaps not so if Parliament retains sovereignty to amend or repeal these rights by normal Parliamentary procedures. This implies that EU27 citizens residing in the UK will not be able to rely on their Charter right whereas

[24] In this paper, as in the Government White Paper, a UK Court, or UK Courts, should be interpreted as a Court or Courts of the constituent jurisdictions of the UK - i.e. England & Wales, Scotland or Northern Ireland.
[25] Case C‑131/12, 25 June 2013, ECLI:EU:C:2013:424 (AG Opinion) and 13 May 2014 ECLI:EU:C:2014:317 (Judgement) both reported at [2014] 3 CMLR 50.
[26] Ibid, [AG119] emphasis added.

EU27 citizens in EU27 member states will be able to so do. This is more than a semantic difference as the UK seemingly seeks a hard Brexit beyond the jurisdiction of the ECJ and quite possible the EFTA Court.

It may be argued that this is moot due to the line of authority that may be drawn from *S. and Marper v. the United Kingdom*.[27] As was famously held in that case

> The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding. However, in determining whether the personal information retained by the authorities involves any of the private-life aspects mentioned above, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained.

This line of authority also encompasses *LH v. Latvia,*[28] *Uzun v. Germany*,[29] and earlier cases such as *X v Germany*.[30] This extensive definition of right to a private life clearly covers data privacy. Thus in *Marper* the data in question were entries on the police database of a database of fingerprints, cell samples and DNA profiles. In *LH* the data were personal medical data collected by the Inspectorate of Quality Control for Medical Care and Fitness for Work ("MADEKKI"). In *Uzun*

[27] [2008] ECHR 1581.
[28] [2014] ECHR 515.
[29] [2011] 53 EHRR 24.
[30] (8334/78) May 7, 1981. Available from: http://hudoc.echr.coe.int/eng-{"appno":["8334/78"]}

the data were gathered GPS data while in *X* the data were documents which had been photocopied in the applicant's office. Clearly this line of authority suggests that the UK's failure to implement Article 8 of the EU Charter is less significant given the expansive interpretation the ECtHR has given to Article 8 of the ECHR for as long as the UK remains a member of the ECHR.

However there are key differences between Article 8 of the EU Charter and Article 8 of the ECHR. By Article 8 of the EU Charter not only does the data subject retain the right to protection of personal data concerning him or her, they also are given a number of subsidiary rights which are not clearly given in Article 8 of the ECHR. Thus by Article 8 of the ECHR the only guarantees given to the data subject are that:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

This is very limiting for it is only interference by a public authority that engages the convention right.[31] The answer would appear to be the principle of horizontality, but as a number of authors, including Phillipson, have noted in determining horizontality: "the issue appears to have been placed firmly in the

[31] The author is acutely aware of significant commentary and case-law on the Horizontal Effect of the ECHR in UK law including Gavin Phillipson, 'The Human Rights Act, "Horizontal Effect" and the Common Law: a Bang or a Whimper?' (1999) 62 MLR 824 and Ian Loveland, 'Horizontality of Art 8 in the context of possession proceedings' (2015) *European Human Rights Law Review* 138. There is insufficient space here to discuss horizontality in full.

keeping of the courts",[32] and recently in an Article 8 application in *McDonald v McDonald*[33] the Court of Appeal ruled that Art 8 does not have horizontal effect in the context of possession proceedings. This means that it is not clearly settled that the expansive definition of Article 8 ECHR would apply horizontally between private citizens in the UK legal systems. By comparison Article 8 of the EU Charter does have horizontal effect as afforded clearly by Article 8(2), and as recognised recently by the Court of Appeal in *Vidal-Hall v. Google Inc*.[34] Further Article 8 of the Charter gives two additional rights, the right to data access and rectification and the right to have reference to a supervisory authority. At risk of labouring the point, these rights will not be retained as *rights* post Brexit. The UK's data protection regime may be compliant but the right to data access and rectification and the right to have reference to a supervisory authority will be lost. Also lost will be the guarantee of horizontal effect and recognition. The existence of the expansive interpretation of Article 8 ECHR found in *Marper* and other cases is not a solution to this problem.

Despite the UK's continuing commitment, at least in the short term, to the ECHR it can therefore clearly be argued that a UK court will still not have the a direct correspondent to Article 8 of the EU Charter in retained UK domestic law against which a court may interpret challenges to UK data protection law.[35] This is a

[32] Phillipson, ibid, 849.
[33] [2014] EWCA Civ 1049.
[34] [2015] EWCA Civ 311.
[35] See further cl.6(3) of the European Union (Withdrawal) Bill 2017-19: 'Any question as to the validity, meaning or effect of any retained EU law is to be decided, so far as that law is unmodified on or after exit day and so far as they are relevant to it— (a) in accordance with *any retained case law and any retained general principles of EU law*.' (emphasis added).

position that may prove a happy resolution to some in the UK. As Mostyn J observed in the case of *AB*:[36]

> The claimant here asserts a violation of article 8 of the Charter of Fundamental Rights of the European Union. This right to protection of personal data is not part of the European Convention on Human Rights, and has therefore not been incorporated into our domestic law by the Human Rights Act. But by virtue of the decision of the court in Luxembourg, and notwithstanding the terms of the opt-out, the claimant is entitled, as Mr Westgate QC correctly says, surprising though it may seem, to assert a violation of it in these domestic proceedings before me.[37]

Against this backdrop, it almost seems an understatement to say, as Orla Lynskey does, "the Charter has been accepted in the UK legal order only with great reluctance".[38] This point was taken up by Marina Wheeler QC who noted that "anxious that the Charter should not be used to overturn national law, the (then Labour) government negotiated what they believed to be an opt out of the Charter by means of Protocol No 30"[39] but that by 2013, and the *AB* decision, the position had been reversed such that as observed by Mostyn J "that much wider Charter of Rights would remain part of our domestic law even if the Human Rights Act were repealed".[40]

---

[36] *AB, R (on the application of) v Secretary of State for the Home Department* [2013] EWHC 3453.
[37] Ibid, [16].
[38] Orla Lynskey, 'Courts, privacy and data protection in the UK: Why two wrongs don't make a right' in M. Brkan and E. Psychogiopou (eds.), *Courts, Privacy and Data Protection in the Digital Environment*, 2017, 215, 229.
[39] Marina Wheeler, 'Cavalier with our Constitution: a Charter too far', UK Human Rights Blog, 9 February 2016: https://ukhumanrightsblog.com/2016/02/09/cavalier-with-our-constitution-a-charter-too-far/ (visited 22 May 2017).
[40] Above n.36, [14].

Ironically of course Brexit reverses this position and the UK finds itself divorced from the Charter but not from the ECHR. The importance of the Charter in UK Law as a source of fundamental rights, including the Article 8 right, may be seen in a number of cases including *Vidal Hall v Google*[41] and *Viagogo*.[42] This vital source of the fundamental data protection right is likely to be lost if the judgement in *AB* is to be followed. We could end up in a zero-sum game where as far as the UK Government is concerned the equivalent of Article 8 is to be found in the UK implementing legislation giving effect to the GDPR, but where there is no Charter right with which to interpret obligations under the UK Legislation. The EU27 may see that as a failure to implement broadly equivalent protections for EU citizens.[43]

Further, a vitally important take-away from the *Google Spain* case is that interpretation of enabling frameworks within Charter rights may even extend our understanding of the enabling provisions. Advocate General Jääskinen believed that "[Article 8] being a restatement of the EU and Council of Europe acquis in this field, emphasises the importance of protection of personal data, but it does not as such add any significant new elements to the interpretation of the Directive"[44] leading him to conclude that "The rights to erasure and blocking of data, provided for in Art.12(b) , and the right to object, provided for in Art.14(a), of Directive 95/46 , do not confer on the data subject a right to address himself

[41] Above n.34.
[42] *The Rugby Football Union v Consolidated Information Services Ltd* [2012] UKSC 55.
[43] At this point it may be further noted that even if one were to accept the expansive interpretation of Art.8 ECHR as being equivalent to Art.8 of the Charter there would be less strong enforceability and a less effective remedy available under the ECHR than under the Charter.
[44] Above n.25, [AG113].

to a search engine service provider in order to prevent indexing of the information relating to him".[45] The Court though disagreed:

> The data subject may, in the light of his fundamental rights under Arts 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name.[46]

The essential difference in Advocate General Jääskinen's approach and that of the Court is the Court's willingness to interpret the Directive expansively in light of Charter rights, including Article 8, which they see as overriding. A UK court post-Brexit (assuming there is to be no "right" to data protection implemented elsewhere) would be unable to do so. This returns us to Baroness Janke's question and Recital 41. It will in all likelihood be impossible for a domestic UK court to interpret "a legal basis or a legislative measure…in accordance with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights" where the fundamental Right to Data Protection found in Article 8 is in question for there will be no domestic equivalent. This appears to be the case due to the current wording of cl.6(3)(a) of the European Union (Withdrawal) Bill (subject to amendment). There it states that in interpreting retained EU Law any court or tribunal must decide the

[45] Ibid, [AG138(3)].
[46] Ibid, [99].

validity, meaning or effect of any retained EU law "so far as that law is unmodified on or after exit day and so far as they are relevant to it *in accordance with any retained case law and any retained general principles of EU law*" (emphasis added). As, as has been previously argued, there will be no retention of Article 8 of the EU Charter they will not be able to refer to Article 8 as it is not a "retained general principle of EU law."

III: GDPR AND ADEQUACY

The UK Government seems to be of the opinion that as part of the Article 50 negotiations the EU27 will recognise the UK implementation of the GDPR (and related provisions including the Law Enforcement Directive[47]) as being suitable for an adequacy decision under Article 45 GDPR or some form of equivalent measure adopted as part of a bilateral treaty or agreement negotiated as part of the Article 50 process. As noted above the Government is quite coy on how this might be achieved with the Minister of State for Digital and Culture refusing to be drawn on whether an adequacy decision was necessary. This seems to suggest the UK will seek to negotiate this as part of the Article 50 settlement.

While we are somewhat in uncharted waters with the Article 50 process which rather baldly states "the Union shall negotiate and conclude an agreement with that State, setting out the arrangements for its withdrawal, taking account of the framework for its future relationship with the Union", what is clear though is that the EU27 cannot agree to anything which would be against EU Law as part

[47] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L 119/89.

of the Article 50 settlement with the UK. The agreement itself, as a new International Treaty enacted by the EU Institutions, would be subject to a possible legality challenge before the ECJ in so far as the EU Institutions cannot act in a way that breaches primary law, including the Charter.[48] This position has recently been confirmed by the CJEU in the *Opinion 1/15* judgement.[49] This judgment is instructive in several ways to this analysis. Firstly it confirms that in place of an adequacy decision the European Union may enter into an international agreement with a third country which allows for the exportation of data to that third country.[50] However, and vital to the current analysis, the Court found that any independently negotiated agreement (as under Article 50) must meet the same adequacy standards as Article 45 agreements.[51] Perhaps equally as importantly the Court reminded us that where data is transferred to a third country, whether under an Article 45 adequacy ruling or under an independently negotiated agreement the third country must also take steps to prevent exportation of that data to countries which fail to provide EU level protection to personal data.[52]

[48] Case C–402/05 P and C–415/05, *Kadi and Al Barakaat International Foundation v Council and Commission* 3 September 2008, ECLI:EU:C:2008:461, [2008] ECR I–6351.
[49] Opinion procedure 1/15, Request for an Opinion pursuant to Article 218(11) TFEU, made on 30 January 2015 by the European Parliament, 26 July2017, ECLI:EU:C:2017:592.
[50] At [214] the Court concludes that "disclosure requires the existence of either an agreement between the European Union and the non-member country concerned equivalent to that agreement, or a decision of the Commission, under Article 25(6) of Directive 95/46, finding that the third country ensures an adequate level of protection within the meaning of EU law and covering the authorities to which it is intended PNR data be transferred."
[51] Ibid, [67]. Further at [214] the Court notes that "a transfer of personal data from the European Union to a non-member country may take place only if that country ensures a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union."
[52] Ibid, [134], [214].

Legally post Brexit the UK will be classified as a "third country" in GDPR terms, whether or not an agreement for data transfers is negotiated as an adequacy decision or as an independent agreement as part of the Article 50 negotiations. The impact of this is that any agreement, whether negotiated as part of the Article 50 settlement or separately must according to the decisions in both *Kadi* and *Opinion 1/15* meet existing EU legal standards and frameworks. This means that any agreement entered into by the UK Government and the EU27 member states will need to comply with Chapter V/Article 44 of the GDPR.

Assuming the UK will not be an EEA state, a position held by the UK Government,[53] then transfers to the UK from the EEA post-Brexit will need to be authorised by one of the suite of available GDPR options. The most likely outcome is an Article 50 treaty or settlement agreed under the same legal framework as the GDPR. Alternatives include a stand-alone adequacy ruling under Article 45, or that transfers be permitted subject to safeguards under Article 46, or be made subject to Binding Corporate Rules under Article 47. These seem to be the only options, as derogations under Article 49 could not apply in all cases. Of the remaining GDPR-compliant provisions (remembering that applying the decisions of the Court in *Kadi* and *Opinion 1/15* agreements made as part of the Article 50 negotiations would need to be GDPR compliant)[54] we find that Article 47 does not create a blanket right for "the unhindered flow of data between the UK and the EU" that the UK Government is seeking so it seems

[53] A UK Government Spokesperson is recorded as saying "The UK is party to the EEA agreement only in its capacity as an EU member state. Once the UK leaves the EU, the EEA agreement will automatically cease to apply to the UK" in L. Hughes and J. Eysenck 'What is the new article 127 Brexit challenge – and what does it mean?' *Daily Telegraph* 2 February 2017: http://www.telegraph.co.uk/news/0/article-127-new-brexit-legal-challenge-single-market/

[54] Above n.48 and n.51.

it can be discounted. This leaves two options "transfers subject to appropriate safeguards" under Article 46 or "transfers on the basis of an adequacy decision" under Article 45.

If the UK believes that an adequacy decision may not be required then this may suggest that the Government believes that transfers may take place under some form of master agreement under Article 46. This provides that "a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available." A safeguards settlement though could not possibly be negotiated during Article 50 negotiations as the undertaking must be given by the controller or processor and cannot be given by the supervisory authority. Although supervisory authorities may authorise standard data protection clauses or approved codes of conduct, agreement would have to be reached individually with data controllers or processors. This means Article 46 cannot be employed to achieve the Government's aims.

We are therefore by process of elimination left with Article 45 either as a stand-alone adequacy decision, or some form of equivalent adequacy settlement independently negotiated under the Article 50 process. The UK Government seems though unwilling to acknowledge this publicly. From the current mood in Westminster it may be assumed that the Government is seeking to put in place an adequacy-equivalent decision as part of the Article 50 negotiations. In fact it may be argued that this position has been publicly acknowledged in the Article

50 letter itself. There the Prime Minister wrote: "leading in the world, and defending itself from security threats … We therefore believe it is necessary to agree the terms of our future partnership alongside those of our withdrawal from the European Union."[55] This is clearly a (not very) veiled reference to the UK's excellence in signals intelligence (SIGINT) data gathering and the need to share data for law enforcement purposes, a point she returned to later in the letter saying, "in security terms a failure to reach agreement would mean our cooperation in the fight against crime and terrorism would be weakened."[56] It seems a data sharing agreement, which one imagines would include an adequacy decision, is explicitly going to be part of the Article 50 negotiations. As a result it may be concluded that the UK is seeking to enter into an independent agreement with the EU27 member states to allow for the free flow of data post Brexit. Such agreement will be required to be in compliance with Article 45 principles for the reasons set out in *Opinion 1/15*.

What will a UK adequacy-standard agreement look like though? At first glance it would seem pretty straightforward, for as Baroness Williams suggests, "on the day that we leave our laws are compatible with those of the EU",[57] however as we have seen subsequently this is not the case both institutionally and constitutionally. The CJEU will no longer have authority over the domestic UK legal settlement, the EU Charter, and in particular Article 8, will have no direct equivalent in UK law and the 105 references to the Commission will have been

[55] Prime Minister's letter to Donald Tusk triggering Article 50: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/604079/Prime_Ministers_letter_to_European_Council_President_Donald_Tusk.pdf
[56] Ibid.
[57] Above, n.5.

excised from (or will be meaningless in) the UK legislation giving effect to GDPR, and the UK will be withdrawn from the European Data Protection Board. In short it is far from as simple as Baroness Williams suggests.

Happily the UK's implementation of GDPR and related Directives will ensure that the UK will meet most, if not all, Article 45 requirements on day one. It will possess clearly an effective supervisory authority in the form of the Information Commissioner's Office, which will have equivalent powers and responsibilities to other EU27/EEA supervisory authorities. It will have similar international commitments to its EU27/EEA partners and will still, at least at the outset, be party to the ECHR; the leading regional system for the protection of privacy aspects of personal data. The UK will possess the necessary legal framework for the recognition of the rights of data subjects and will have an effective and functioning system for effective and enforceable administrative and judicial redress for the data subjects whose personal data are being transferred. When one compares for example the position of the UK on 29 March 2019 with the position of a number of countries which have adequacy decisions such as Switzerland, Uruguay or the Privacy Shield agreement with the federal government of the United States it is clear the UK will have a much more comprehensive and compliant data protection regime. The UK should therefore qualify immediately for an adequacy-standard agreement. However there is one UK legal provision which may prove problematic both in the short-term and in the longer term.

IV: THE INVESTIGATORY POWERS ACT 2016

The Investigatory Powers Act 2016 is a comprehensive restatement of UK security and intelligence laws. It covers a variety of law enforcement and investigatory techniques employed by the police and by the security and intelligence services from interception of communications to equipment interference and covers a wide range of targeted and bulk warrants.

For the purposes of this paper we will focus on Part 4: Retention of Communications Data. This part of the Act permits data retention orders to be issued, replacing the provisions of the now repealed Data Retention and Investigatory Powers Act 2014 (DRIPA). The effective power is found in s.87(1). This permits the "Secretary of State [to] require a telecommunications operator to retain relevant communications data if (a) the Secretary of State considers that the requirement is necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (j) of section 61(7) (purposes for which communications data may be obtained), and (b) the decision to give the notice has been approved by a Judicial Commissioner." The key difference between s.87(1) and s.1(1) of DRIPA is the addition of sub-section (b): oversight by a Judicial Commissioner. The list of permitted purposes found in s.61(7) is at first glance wider than that permitted under DRIPA. New permitted purposes include: (a) to assist investigations into alleged miscarriages of justice; (b) to assist in the identification of a person or their next of kin and (c) functions relating to the regulation of financial services and markets, or financial stability. Some purposes have been removed or narrowed, offsetting some of the new purposes. Thus the previously permitted purpose of "in the interests of the economic well-being of

the United Kingdom" has been narrowed by the addition of qualifying text "so far as those interests are also relevant to the interests of national security" while a general law-making power "for any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State" is removed. This final amendment, alongside the role of the Judicial Commissioners may assist the UK Government in securing an adequacy decision, although as we shall see this is far from certain.

Significant new safeguards have been added. By s.88 the Secretary of State must take a reflective overview of the need to issue a retention notice before it is issued taking into account (among others): the likely benefits of the notice, the likely number of users (if known) of any telecommunications service to which the notice relates, the technical feasibility of complying with the notice, and the likely cost of complying with the notice. Further by s.88(2) the Secretary of State must, before giving such a notice, take reasonable steps to consult any operator to whom it relates. The second additional safeguard is the addition of the review of the Judicial Commissioners. The role of the Judicial Commissioners is new and may be found in s.227. This creates the new positions of the Investigatory Powers Commissioner and other Judicial Commissioners. The Investigatory Powers Commissioner is the chief Judicial Commissioner and must have held high judicial office (as must the other Judicial Commissioners). Lord Justice Fulford, Senior Presiding Judge for England and Wales, has been appointed as the first Investigatory Powers Commissioner.[58] The Judicial Commissioners are

[58] Her Majesty's Government, *Press Release Investigatory Powers Commissioner Appointed: Lord Justice Fulford*, 3 March 2017. Available from:

charged under s.89(1) to "review the Secretary of State's conclusions as to whether the requirement to be imposed by the notice to retain relevant communications data is necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (j) of section 61(7)." However the way they are to do this is rather unusual. By s.89(2)(a) they are directed to "apply the same principles as would be applied by a court on an application for judicial review" while by s.89(2)(b) they are required to "consider the matters referred to in subsection (1) with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy)."

These two provisions seem to be in conflict. The duties imposed by section 2 ask the Commissioners to weigh: (a) whether what is sought to be achieved by the warrant, authorisation or notice could reasonably be achieved by other less intrusive means; (b) whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant, authorisation or notice is higher because of the particular sensitivity of that information; (c) the public interest in the integrity and security of telecommunication systems and postal services; and (d) any other aspects of the public interest in the protection of privacy against (a) the interests of national security or of the economic well-being of the United Kingdom, and (b) the public interest in preventing or detecting serious crime. However this solemn weighting of privacy against the public interest is somewhat undermined by the s.89(2)(a) requirement that the

---

https://www.gov.uk/government/news/investigatory-powers-commissioner-appointed-lord-justice-fulford

Judicial Commissioners "apply the same principles as would be applied by a court on an application for judicial review".

Judicial review principles are rather narrow and review the administrative process of the decision rather than the substance of the decision. This means commissioners will be restricted in the scope of their actions to the three Judicial Review grounds: (1) Illegality: conflict with legal order or *ultra vires*; (2) Fairness: a public body should never act so unfairly that it amounts to an abuse of power; and (3) Irrationality and proportionality: a decision may be considered so demonstrably unreasonable as to constitute 'irrationality' or 'perversity' on the part of the decision maker.

Some have criticised the adoption of judicial review principles. Appearing before the Joint Committee on the Draft Investigatory Powers Bill Caroline Wilson Palow, General Counsel of Privacy International, argued that "the Judicial Commissioners need the full ability to assess the warrants when they come to them. It should not be just a judicial review standard. They need to assess fully the substance of the warrant and, among other things, whether there are other less obtrusive means by which this information could be obtained."[59] Shami Chakrabarti, then Director of Liberty, was more forceful.

> Judicial review does not help at all in this context. When you are deciding whether it is proportionate to issue a warrant for intrusive surveillance of an individual, let alone of a whole group of people, that

[59] Joint Committee on the Draft Investigatory Powers Bill, Oral evidence: Draft Investigatory Powers Bill, HC 651, Wednesday 9 December 2015: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/oral/25977.html

> is a judgment made on the evidence. A judicial review test only second-guesses the Secretary of State, in very limited circumstances. Did they make a bonkers decision that no reasonable Secretary of State could take?[60]

Others take a more sympathetic view to the use of Judicial Review standards. Lord David Pannick QC in an article for *The Times* newspaper noted that "Andy Burnham and David Davis…say that a judicial review test gives judges too little power because it only relates to 'process'. But it is well established that judicial review is a flexible concept, the rigour of which depends on the context. The Court of Appeal so stated in 2008 in the T-Mobile case."[61] He goes on to point out that Judges already apply Judicial Review standards successfully in a complex rights framework.

> [t]he closest analogy to the provisions in the draft bill is judicial review of control orders and Tpims (terrorist prevention and investigation measures). The Court of Appeal stated in the MB case in 2006 that judges applying a judicial review test must themselves consider the merits and decide whether the measure is indeed necessary and proportionate. It is true that the context there involves restrictions that vitally affect liberty — in the sense of freedom of movement. But I would expect the courts to apply a very similar approach in the present context, concerned as it is with the important issue of privacy. So those who are concerned that a

[60] Ibid.
[61] David Pannick QC: 'Safeguards provide a fair balance on surveillance powers' *The Times* 12 November 2015. The T-Mobile case refereed to is *T-Mobile & Telefonica v Ofcom* [2008] EWCA Civ 1373.

judicial review test does not give judges sufficient control should be reassured.[62]

Sir Stanley Burnton, then Interception of Communications Commissioner, and Lord Judge, then Chief Surveillance Commissioner, both endorsed the Pannick approach, however not without reservation. In their evidence to the Joint Committee on the Draft Investigatory Powers Bill Sir Stanley noted that "Judicial review is not simply a question of looking at process. [T]he commissioner has to look at necessity and proportionality. The degree to which judicial review is imposed as a test and the stringency of the test depend very much on the context, the facts of the individual case and the consequences of the administrative or governmental decision in question."[63] Lord Judge supported Sir Stanley's position but added a hesitation.

> My only hesitation, which is a lawyerly one but not totally without some force, is in using the words 'judicial review' as a description of the test that has to be applied by the judicial officer. Judicial review used to be Wednesbury unreasonable mad. We would call it Wednesbury unreasonable, meaning only an idiot could have reached this decision. Nowadays, judicial review is less stringent than that: 'He is not an idiot, but it is a really stupid decision'. That is not quite the same. 'I am not sure many people would have reached this decision' is another test. We need to be slightly careful. If you are talking about the Home Secretary…[t]he

[62] Ibid.
[63] Joint Committee on the Draft Investigatory Powers Bill, Oral evidence: Draft Investigatory Powers Bill, HC 651, Wednesday 2 December 2015: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/oral/25685.html

> Home Secretary has the most amazing responsibilities in relation to that. Judges second guessing is simply inappropriate. You have to have a stringent judicial review test. I am now coming back to what Sir Stanley said. You know you are dealing with national security; you know somebody might be planting a bomb. You are going to be very cautious about interfering and saying, 'This man or woman, who is the Secretary of State, is daft'.[64]

Lord Judge's hesitation raises a note of concern that may impact the UK's ability to obtain an equivalency decision. The draft of the Bill being discussed in Committee on that date did not contain a provision equivalent to s.89(2)(b). Some may argue the addition of s.89(2)(b) will empower Judicial Commissioners to take the expansive Pannick view that will employ "a judicial review test [which] must [] consider the merits and decide whether the measure is indeed necessary and proportionate" however if as he says "judicial review is a flexible concept, the rigour of which depends on the context" then the risk is that when s.89(2)(a) and 89(2)(b) are placed in conflict Judicial Commissioners will follow the Judge line that warrants should only be refused when the Commissioner believes that "this man or woman, who is the Secretary of State, is daft." This could have far reaching implications for the recognition of adequacy in UK data protection law post Brexit due to the line of authority of *Digital Rights Ireland Ltd v Minister for Communications*,[65] *Maximillian Schrems v Data Protection Commissioner*[66] and *Tele2 Sverige AB v Post-och telestyrelsen*.[67]

[64] Ibid.
[65] Joined Cases C‑293/12 and C‑594/12, 8 April 2014, ECLI:EU:C:2014:238.
[66] Case C-362/14, 6 October 2015, ECLI:EU:C:2015:650.

V: *DIGITAL RIGHTS IRELAND LTD v. MINISTER FOR COMMUNICATIONS*[68]

The *Digital Rights Ireland* case was, of course, was the famous challenge to the now repealed Data Retention Directive.[69] While the long-term legal impact of the case is reduced due to the fact that it was a specific challenge to the Directive's legality there are still a number of important take-aways for a post-Brexit data protection environment.

While much of the detail of the case turned upon the interplay between Article 15(1) of the ePrivacy Directive,[70] Article 13(1) of the Data Protection Directive[71] and the provisions of the Data Retention Directive,[72] there were elements of interplay also with the EU Charter and the rights framework of the EU. Vitally the Court found

> The retention of data for the purpose of possible access to them by the competent national authorities, as provided for by Directive 2006/24, directly and specifically affects private life and, consequently, the rights guaranteed by Article 7 of the Charter. ***Furthermore, such a retention of data also falls under Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and,***

[67] Joined Cases C-203/15 and C-698/15, 21 December 2016, ECLI:EU:C:2016:970.
[68] Above n.65.
[69] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ 2006 L 105/54.
[70] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ 2002 L 201/37.
[71] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 2005 L 281/31.
[72] Above, n.69.

therefore, necessarily has to satisfy the data protection requirements arising from that article.[73]

This is important as it confirms that data retention processes engage Article 8 of the EU Charter and as we have seen above Article 8 is one of the provisions of the Charter not to have guaranteed recognition in the UK in the post-Brexit environment. Now, as we have already rehearsed, an argument may be made that by importing the GDPR framework into domestic UK law in full then the UK will have satisfied "the data protection requirements arising from that article". However a contrary interpretation is that, again as we have seen, when the UK leaves the EU, UK citizens (and EU citizens looking to enforce in the UK) will lose their right to data protection as found in Article 8. They will, as set out above, retain only the shadow of the right through the framework for data protection found in the UK implementation of the GDPR.

In *Digital Rights Ireland* the court found that "Directive 2006/24 constitutes an *interference* with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter because it provides for the processing of personal data."[74] This is an important development. The Court clearly states that data retention not only engages Article 8, it is also an interference with the fundamental right to data protection. The question then comes down to whether or not that interference is justified. After quickly finding that "the retention of data for the purpose of allowing the competent national authorities to have possible access to those data, as required by Directive 2006/24, genuinely

[73] *Digital Rights Ireland Ltd v Minister for Communications*, above n.65, [29] (emphasis added).
[74] Ibid, [36] (emphasis added).

satisfies an objective of general interest"[75] that interest being "the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest and the fight against serious crime in order to ensure public security"[76] the Court moved on to the question of proportionality.

Here the Court found that "in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by Directive 2006/24, the EU legislature's discretion is reduced, with the result that review of that discretion should be strict."[77] The Court further noted, "the protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is especially important for the right to respect for private life enshrined in Article 7 of the Charter."[78] As a result of this "the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data."[79] Finding that the Directive required all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony to be retained the Court found the

[75] Ibid, [44].
[76] Ibid, [42].
[77] Ibid, [48].
[78] Ibid, [53].
[79] Ibid, [54].

Directive not to be a proportionate response to the threat and struck it down. In so doing the Court ruled:

> Directive 2006/24 does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. In the first place, Article 7 of Directive 2006/24 does not lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality.[80]

The risk of this decision to the post-Brexit flow of data between the EU27/EEA and the UK is clear. The Investigatory Powers Act does not have these protections. Section 2, as implemented in data retention cases by s.89(2)(b), asks the Judicial Commissioners to consider "whether what is sought to be achieved by the warrant, authorisation or notice could reasonably be achieved by other less intrusive means" and "whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant, authorisation or notice is higher because of the particular sensitivity of that information". In addition by s.92 "a telecommunications operator who retains relevant communications data must (a) secure that the data is of the same integrity, and subject to at least the same security and protection, as the data on any system

[80] Ibid, [66].

from which it is derived, (b) secure, by appropriate technical and organisational measures, that the data can be accessed only by specially authorised personnel, and (c) protect, by appropriate technical and organisational measures, the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful retention, processing, access or disclosure." The Government believes that collectively these represent implementation of data protection provisions for retained data. Essentially if the system was data protection compliant when the data were gathered then it will remain so under s.92(1)(a) while retained. However there are two problems with this. The first is that this appears to be far short of "govern[ing] the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality." The second is that it assumes the data retained were in a compliant system at the point it was retained. Currently this would be subject to a challenge that engages Article 8 of the EU Charter. Post-Brexit this will not be possible.

VI: TELE2 SVERIGE AB v. POST-OCH TELESTYRELSEN

Two UK MPs, David Davis MP (now ironically Secretary of State for Exiting the European Union) and Tom Watson MP brought a challenge to the UK's subsequent domestic legislation, the Data Retention and Investigatory Powers Act 2016 (DRIPA). The reference to the CJEU from the UK Court of Appeal was joined with a Swedish reference *Tele2 Sverige AB v Post-och telestyrelsen*.[81] Davis and Watson (later just Watson as Davis's appointment to the UK Cabinet placed

[81] Above n.67.

him in conflict and he was required to drop out of the challenge) argued that the Digital Rights Ireland judgment laid down "mandatory requirements of EU law" applicable to the legislation of Member States on the retention of communications data and access to such data. This meant that the provisions of DRIPA, which broadly replicated the provisions of the Data Retention Directive (though subject to a "retention notice" issued under s.1(1) by the Secretary of State rather than as a blanket retention as the Directive had provided), were unlawful under EU law. The Divisional Court agreed finding that as the Data Retention Directive was incompatible with the principle of proportionality, national legislation containing the same provisions as that Directive could, equally, not be compatible with that principle.[82] The Government appealed and the Court of Appeal took a different interpretation taking a provisional view that, in *Digital Rights Ireland*, the Court of Justice was not laying down specific mandatory requirements of EU law with which national legislation must comply, but was simply identifying and describing protections that were absent from the harmonised EU regime, while referring the case to the CJEU.[83]

The Court of Appeal referred two questions to the CJEU:

> (1) Did the CJEU in Digital Rights Ireland intend to lay down mandatory requirements of EU law with which the national legislation of Member States must comply?

[82] *R .v Secretary of State for the Home Department (ex parte Davis & Watson)* [2015] EWHC 2092 (Admin).
[83] *Secretary of State for the Home Department v Davis and Ors.* [2015] EWCA Civ 1185.

(2) Did the CJEU in Digital Rights Ireland intend to expand the effect of Articles 7 and/or 8, EU Charter beyond the effect of Article 8 ECHR as established in the jurisprudence of the ECtHR?[84]

When the cases were joined the CJEU slightly altered the approach to the questions but the key questions of whether the *Digital Rights Ireland* case laid requirements on member states, and what the correct approach to the application of Articles 7 and 8 were, remained.

Like the *Digital Rights Ireland* case much of the discussion both in Advocate General Saugmandsgaard Øe's and in the Court's opinion turned on technical issues of the interplay of the EU legal framework. The key question here was whether the existence of the data retention provision found in Article 15(1) of the ePrivacy Directive precluded member states from making domestic legislation in this area without reference to Article 15(1). As such the argument of the claimants was that domestic legislation made under Article 15(1) would be bound by the principles of Digital Rights Ireland. This is a very interesting and important point but not directly relevant to this analysis so will not be pursued further here.[85]

[84] Ibid, [118].

[85] Although not relevant to this analysis this point is very important for the Brexit position of the Investigatory Powers Tribunal (IPT). If the IPT upholds this point they may find that the EU did not have competence to act in national security matters and post Brexit any EU provisions are inapplicable. This in itself is not an issue for an equivalence decision as Art.23(1)(a)of the GDPR allows for restrictions. This matter was discussed in *Secretary of State for the Home Department v Davis and Ors*, above n.83, at [91] – [106].

Essential to our analysis here is the interplay between the domestic UK legislation and the UK's responsibilities under the EU Charter. A key point raised by Advocate General Saugmandsgaard Øe in relation to domestic regimes as opposed to a harmonised one, was:

> In accordance with Art.8(3) of the Charter, every Member State must ensure that an independent authority reviews compliance with the requirements of protection and security on the part of the service providers to which their national regimes apply. In the absence of coordination throughout the European Union, however, those national authorities might find it impossible to fulfil their supervisory duties in other Member States.[86]

This is a question likely to be magnified post-Brexit when the UK leaves the EU Charter. In his analysis of whether the Swedish and UK provisions met the requirements of Arts 7 & 8 of the Charter Advocate General Saugmandsgaard Øe observed that an argument made by the UK Government that "a general data retention obligation may be justified by any of the objectives mentioned in either Art.15(1) of Directive 2002/58 or Art.13(1) of Directive 95/46. According to that such an obligation could be justified by the utility of retained data in combating 'ordinary' (as opposed to 'serious') offences, or even in proceedings other than criminal proceedings, with regard to the objectives mentioned in those

[86] Opinion of Advocate General Saugmandsgaard Øe delivered on 19 July 2016 in *Tele2 Sverige AB v Post-och telestyrelsen* (C-203/15) and *Secretary of State for the Home Department v Tom Watson* (C-698/15) ECLI:EU:C:2016:572 at [241].

provisions"[87] was "not convincing". He came to this conclusion for several reasons but prime among them was

> The requirement of proportionality within a democratic society prevents the combating of ordinary offences and the smooth conduct of proceedings other than criminal proceedings from constituting justifications for a general data retention obligation. The considerable risks that such obligations entail outweigh the benefits they offer in combating ordinary offences and in the conduct of proceedings other than criminal proceedings.[88]

The CJEU in their judgement backed Advocate General Saugmandsgaard Øe's interpretation finding that "the objective pursued by that legislation must be proportionate to the seriousness of the interference in fundamental rights that that access entails, it follows that, in the area of prevention, investigation, detection and prosecution of criminal offences, only the objective of fighting ***serious*** crime is capable of justifying such access to the retained data."[89]

This remains a problem for the UK Government. By s.87(1) of the Investigatory Powers Act 2016 the Secretary of State may issue a retention notice if the Secretary of State "considers that the requirement is necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (j) of section 61(7)". These purposes are: (a) the interests of national security; (b) preventing or detecting crime or of preventing disorder; (c) the economic well-being of the United Kingdom so far as those interests are also relevant to the

[87] Ibid, [169].
[88] Ibid, [172].
[89] *Tele2 Sverige AB v Post-och telestyrelsen* (C-203/15) and *Secretary of State for the Home Department v Tom Watson* (C-698/15) above n.67 at [115] (emphasis added).

interests of national security; (d) in the interests of public safety; (e) for the purpose of protecting public health; (f) for assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; (g) for preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; (h) to assist investigations into alleged miscarriages of justice; (i) where a person has died or is unable to identify themselves because of a physical or mental condition to assist in identifying them, or to obtain information about their next of kin or other persons connected with them; (j) for the purpose of exercising functions relating to the regulation of financial services and markets, or financial stability.

Looking at this list only (a), (c) and (d) seem clearly to meet the standard the Court is thinking of. It is possible in certain circumstances that (b) (e) and (j) are compliant, but it is hard to think of cases where (f), (g), (h) and (i) would meet the high *Tele2* standard. Most clearly heading (b) preventing or detecting crime or of preventing disorder does not meet the *Tele2* standard of "only the objective of fighting ***serious*** crime is capable of justifying such access to the retained data".

Additionally the Investigatory Powers Act retains the wide scope of the DRIPA provision, what may be called a "general or indiscriminate" notice. By s.87(2)(a) – (c) a retention notice may "relate to a particular operator or any description of operators", "require the retention ***of all data or any description of data***", and "identify the period or periods for which data is to be retained" (emphasis added). Collectively these provisions suggest notices which can apply to a

particular operator (or a number of operators), may be defined so as to retain all data that operator holds for an extended period. This fits the definition of a "general or indiscriminate" notice that the Court ruled to be incompatible with the Charter in *Tele2*.[90] This suggests a fundamental difference in approach between the UK and the EU27 on this matter.

It is not only the question of purposes which may affect the UK's ability to obtain an adequacy decision post *Tele2*. The question of the UK's supervisory arrangements for retention orders under Part 4 is also questionable. *Tele2* requires:

> Member States [to] ensure review, by an independent authority, of compliance with the level of protection guaranteed by EU law with respect to the protection of individuals in relation to the processing of personal data, that control being expressly required by Art.8(3) of the Charter and constituting, in accordance with the Court's settled case-law, an essential element of respect for the protection of individuals in relation to the processing of personal data. If that were not so, persons whose personal data was retained would be deprived of the right, guaranteed in Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim seeking the protection of their data.[91]

The UK meets this in the Investigatory Powers Act 2016 through s.244: "The Information Commissioner must audit compliance with requirements or

[90] Ibid, [103], [112].
[91] Ibid, [123].

restrictions imposed by virtue of Part 4 in relation to the integrity, security or destruction of data retained by virtue of that Part." However it is certainly not clear that this simple audit role meets the requirement of *Tele2* that "persons have a right, guaranteed in Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim seeking the protection of their data." Individuals who wish to challenge the retention and storage of personal data under a data retention notice must do so through an application to the Investigatory Powers Tribunal (discussed further below). This may only be done in accordance with s.65 of the Regulation of Investigatory Powers Act 2000. This allows for two forms of challenge: a claim under the Human Rights Act 1998 for any breach of fundamental rights; or a complaint against a public authority for using covert techniques. Although providing a remedy, and arguably as will be discussed below, one which is probably GDPR complaint, this is a judicial procedure and seems quite distinct from the role of national supervisory authorities as required by *Tele2*.

In short there are a number of areas where the interaction of the Investigatory Powers Act 2016 and the decision in *Tele2* may find themselves in conflict. These all potentially undermine the UK's ability to receive an adequacy decision under Article 45 GDPR.

VII: SCHREMS

Inevitably when discussing the interplay between data transfers and adequacy decisions one finds themself faced with the *Schrems* decision.[92] This was the

[92] *Maximillian Schrems v Data Protection Commissioner*, above n.66.

famous challenge to the Safe Harbor adequacy decision[93] brought by Austrian student Max Schrems following the Snowden revelations. Mr. Schrems argued, ultimately successfully, that "that the law and practices of the United States offer no real protection of the data kept in the United States against State surveillance."[94]

The potential parallels between the *Schrems* challenge and the UK's desire to have an adequacy ruling post-Brexit are clear. The UK, like the US, operates a massive state surveillance regime involving not only data retention as this paper has discussed at length, but also policies such as TEMPORA, the system used by GCHQ to buffer most Internet communications extracted from fibre-optic cables so these can be processed and searched at a later time. This programme is operated alongside commercial partners such as Vodafone and British Telecommunications making it not unlike the PRISM programme at the heart of the Schrems case.

The key question is, given the previous discussion of the UK's data retention programme, and the decisions in *Digital Rights Ireland* and *Tele2*, could *Schrems* deliver a potentially fatal blow to any attempts by the UK Government to secure a lasting adequacy ruling in the Article 50 negotiations?

[93] European Commission Decision 2000/520 of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ 2000 L215/7.
[94] Opinion of Advocate General Bot delivered on 23 September 2015, Case C-362/14, ECLI:EU:C:2015:627 *Maximillian Schrems v Data Protection Commissioner*, [AG25].

The first thing to note is that by implementing the GDPR in full and given the pre-existence of a supervisory authority in the form of the Information Commissioner's Office the UK sidesteps the main complaint in *Schrems*: the UK has a functional and functioning out of court dispute resolution system operated by an independent third party. However the role of the Information Commissioner's Office is limited in questions of national security.[95] We can assume that in any domestic legislation giving effect to the GDPR the UK Government will seek to continue the exemption the security services currently enjoy through an implementation of the Article 23 GDPR restriction. Currently the UK is shielded from any implication of this restriction by the fact that it is an EU member state and subject to effective supervision via the CJEU with the full force of EU law, including the Charter, in place. When the UK leaves and goes it alone it loses this framework. The Commission in coming to an adequacy decision will be required to apply *Schrems* and this tells us that "legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Art.47 of the Charter."[96] In the *Schrems* case there was insufficient protection of Article 47 for in the words of Advocate General Bot "there is oversight on the part of the FISC, but the proceedings before it are secret and ex parte. I consider that that amounts to an interference with the right of citizens of the Union to an effective remedy, protected by Art.47 of the Charter."[97]

[95] See s.28 of the Data Protection Act 1998.
[96] Above, n.66, [95].
[97] Above, n.94, [173].

Under the Investigatory Powers Act 2016 and the Regulation of Investigatory Powers Act 2000 the only effective route to challenge any decision or action of the security services is the Investigatory Powers Tribunal. The Tribunal is not unlike FISC in that by s.68 of the Regulation of Investigatory Powers Act 2000 it may "determine their own procedure in relation to any proceedings, complaint or reference brought before or made to them". In practice procedure is as stated on the Tribunal's web site.

> We are the first court of our kind to establish 'inter partes' hearings in open court in the security field. These hearings allow us to hear arguments on both sides on the basis of 'assumed facts' without risk to our national security. This means that where there is a substantial issue of law to consider, and without at that stage taking a decision as to whether the allegation in a complaint is true, we invite the parties involved to present issues of law for the Tribunal to decide, which are based on the assumption that the facts alleged in the complaint are true. This means that we have been able to hold hearings in public, including full adversarial argument, as to whether the conduct alleged, if it had occurred, would have been lawful. We may then hold 'closed' hearings in private to apply the legal conclusions from the open hearings to the facts.[98]

This mixture of open inter partes hearings and then closed hearings on the facts may be enough to allow the UK to convincingly argue that the IPT is quite distinct from FISC and therefore the UK is compliant with Article 47.

[98] http://www.ipt-uk.com/ (visited 1 August 2017).

The story doesn't end there though. Perhaps the key outcome of *Schrems* was the clear statement that "legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter."[99] Again the UK has until now been shielded by its EU membership and in particular its membership of the Charter. This time the UK may point to the fact that it remains an ECHR state (at least for the foreseeable future) and as a result for Article 7 of the Charter we may substitute Article 8 ECHR. However it is clear that the Investigatory Powers Act 2016 contains a number of provisions that apply to EU27 residents and citizens in a different manner to "individuals in the British Islands".[100] For example if one looks to s.136, Bulk Interception Warrants we are told that they may only be issued for "the interception of overseas-related communications" and that this is "communications sent by individuals who are outside the British Islands, or communications received by individuals who are outside the British Islands." Similar distinctions may be found in s.158 (Bulk Acquisition Warrants) and s.176 (Bulk Equipment Interference Warrants).[101]

Thus EU27 residents (and presumably overwhelmingly citizens) in the UK will be treated differently under the Investigatory Powers Act to UK residents (and

[99] Above n.66, [94].
[100] The British Islands is a legal definition of collective landmasses found in Schedule 1 of the Interpretation Act 1978. It is "the United Kingdom, the Channel Islands and the Isle of Man."
[101] A discussion of what qualifies as an "overseas-related communication", or in the language of the Regulation of Investigatory Powers Act 2000, an external communication, may be found at *Liberty & Ors. v GCHQ & Ors.* [2014] UKIPTrib 13_77-H. Available from: http://www.ipt-uk.com/docs/IPT_13_168-173_H.pdf (visited 1 August 2017).

overwhelmingly citizens). This makes the *Schrems* statement a live issue. There are safeguards in place, in each case a warrant must be issued by the Secretary of State and must be approved by Judicial Commissioners. It is not therefore "retention on a generalised basis" of communications and communications data but rather some form of targeted system. At least that's what the UK Government would say. However when we also know that GCHQ were using as few as eighteen periodically renewed RIPA s.8(4) warrants to authorise TEMPORA as well as their other programmes,[102] allowing them to tap into the transatlantic fibre optic cables, which reportedly allowed them to processes 40 billion items of data per day: then these safeguards seem more illusory than real. The questions therefore become (a) is this "legislation permitting the public authorities to have access [to communications and data] on a generalised basis" and (b) will the additional safeguards of the Investigatory Powers Act, such as the introduction of Judicial Commissioners, protect the UK Government?

VIII: CONCLUSIONS

The evidence is clearly beginning to mount against the assumption that the UK will be able "to secure the unhindered flow of data between the UK and the EU post-Brexit" as Mr. Hancock would like. Whether negotiated as part of the Article 50 settlement, or separately as an adequacy decision, there are clear issues the UK Government needs to overcome regarding both data retention and mass surveillance. When this is placed against a backdrop of a likely failure of the UK domestic settlement to recognise an Article 8 right to Data Protection (as

[102] Intelligence and Security Committee of Parliament, *Privacy and Security: A modern and transparent legal framework*, HC 1075, 12 March 2015, fn83.

opposed to the operationalization of that right through GDPR style legislation) things begin to look bleak.

When one examines the *Schrems* decision some other issues emerge. The first is that even should an adequacy decision be issued, then as Max Schrems did himself, EU27 citizens concerned about the UK's state surveillance and data retention programme may challenge the transfer of their data to the UK via any EU27 supervisory authority.[103] Secondly the duties of the Commission do not end with an adequacy decision. As the Court stated in *Schrems* "in the light of the fact that the level of protection ensured by a third country is liable to change, it is incumbent upon the Commission, after it has adopted a decision pursuant to Article 25(6) of Directive 95/46, to check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified. Such a check is required, in any event, when evidence gives rise to a doubt in that regard."[104] Further "as the Advocate General has stated in points 134 and 135 of his Opinion, when the validity of a Commission decision adopted pursuant to Article 25(6) of Directive 95/46 is examined, account must also be taken of the circumstances that have arisen after that decision's adoption."[105]

Perhaps of most concern for the UK Government going forward is that such a review must be strict.[106] The possible impact of this is that even if the UK has some form of adequacy decision, whether negotiated as part of the Article 50

[103] Above n.66, [40-41].
[104] Ibid, [76].
[105] Ibid, [77].
[106] Ibid, [78].

settlement, or as a separate Article 45 GDPR ruling, on 29 March 2019 an immediate challenge from a civil society group or individual along the lines of *Schrems* or *Digital Rights Ireland v Commission*[107] is quite likely given the UK's extensive framework of data retention and surveillance legislation, some of which treats EU27 residents (and thereby mostly citizens), differently to residents of the British Islands. It is not impossible that as a result of such a challenge, or even just in the fullness of time as details of how GCHQ and SIS/The Security Service operate under the Investigatory Powers Bill framework,[108] a review of any adequacy decision may be reversed applying the strict *Schrems* criteria.

It is clear that the realpolitik of Brexit is that a continued free flow of data between the EU27 and the UK is in the interests of all parties due to the extensive nature of the digital single market, GCHQ's vital role in SIGINT provision to Europe as a whole and London's continued, though perhaps diminished, role as the world's leading financial centre.[109] This will in all likelihood lead to some form of compromise position being reached before 29 March 2019 that will deliver to the UK the settlement they seek. However this paper suggests that it is folly to assume that the UK's legal framework guarantees this settlement merely by the implementation of the GDPR through domestic legislation. Further, although the position on 29 March 2019 may be that

[107] Case T-670/16, OJ 2016 C 410/26.
[108] On which see Kieren McCarthy, 'Leaked: The UK's secret blueprint with telcos for mass spying on internet, phones – and backdoors. Real-time full-blown snooping with breakable encryption', *The Register*, 4 May 2017: https://www.theregister.co.uk/2017/05/04/uk_bulk_surveillance_powers_draft
[109] On which see Karen McCullagh, "Brexit: potential trade and data implications for digital and 'fintech' industries", 7(1*)* IDPL 3 (2017).

agreement on data transfers has been reached, we cannot assume that position would remain in effect indefinitely given the responsibility of the Commission to "to check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified."[110]

[110] *Maximillian Schrems v Data Protection Commissioner,* above n.66 at [64].