THE HIGH COURT
JUDICIAL REVIEW

Record No.: 2013/765 JR

Between:-

MAXIMILLIAN SCHREMS

Applicant

-and-

DATA PROTECTION COMMISSIONER

Respondent

OUTLINE SUBMISSIONS ON BEHALF OF THE RESPONDENT

Contents

A) Introduction.

1) On 25 June 2013 the Applicant made a complaint to the Respondent concerning what has been referred to as the "PRISM" programme and its application to arrangements under which Facebook Ireland Limited transfers personal data relating to Facebook subscribers resident in the European Economic Area to the United States, to be held there on servers controlled by its parent company, Facebook Incorporated.

2) The Respondent declined to investigate the said complaint having formed the opinion ("the impugned opinion") that it was frivolous or vexatious within the meaning of Section 10(1)(b)(i) of the Data Protection Acts 1988-2003 ("the DP Acts"). In these proceedings, the Applicant challenges the impugned opinion.

3) In ***Nowak v Data Protection Commissioner*** [2013] 1 ILRM 207 Birmingham J explained the nature of an opinion formed under Section 10(1)(b)(i) in the following terms:

> *"Once the Commissioner had formed the view that the examination script did not constitute personal data it followed that he was being asked to proceed with an investigation where no breach of the Data Protection Acts could be identified. It was in those circumstances he had resort to s. 10(1)(b)(i). That section refers to complaints that are frivolous or vexatious. However, I do not understand these terms to be necessarily pejorative. Frivolous, in this context does not mean only foolish or silly, but rather a complaint that was futile, or misconceived or hopeless in the sense that it was incapable of achieving the desired outcome, see R. v. North West Suffolk (Mildenhall) Magistrates Courts Ex P Forest Heat D. C. [1997] EWCA Civ 1575, unreported Court of Appeal, May 16,1997.. Having regard to the view the Commissioner had formed that examination scripts did not constitute personal data, he was entitled to conclude that the complaint was futile, misconceived or hopeless in the sense that I have described, indeed such a conclusion was inevitable"* (page 216)(emphasis added).

4) The desired outcome that the Applicant sought is apparent from his original letter of complaint dated 25 June 2013 in which he demanded the following of the Respondent:

(i) That he review the validity of Commission Decision No. C2000/520/EC ("the Commission Decision"), which in turn incorporates the Safe Harbour Privacy Principles and FAQs;

(ii) If necessary, that he obtain a preliminary ruling from the European Court of Justice on the validity of the Commission Decision; and

(iii) If necessary, that he prohibit the transfer of personal data to Facebook Inc unless Facebook Ireland Ltd could disprove reports of arrangements under which it was alleged that national security services in the United Stated were in a position to obtain direct and unhindered access to bulk data held on servers located in that jurisdiction relating to Facebook subscribers resident in the European Economic Area.

5) The Respondent formed the opinion that the Applicant's complaint should not be admitted for investigation because, in light of (a) Section 11 of the DP Acts; (b) the Commission Decision; (c) the terms of the Safe Harbour Privacy Principles and FAQs; and (d) Facebook's self-certified adherence to the Safe Harbour Principles and FAQs (such certification having been verified by the Respondent's office by examining entries noted on a publicly-accessible register operated by the United States Department of Commerce), the complaint was bound to fail and, as such, was properly to be considered "frivolous or vexatious" within the meaning of that term as set out at Section 10(1)(b)(i) of the DP Acts.

6) Put simply, the Respondent considered that, in the particular circumstances that obtained, he was statutorily bound to accept that a transfer of subscriber data by Facebook Ireland to Facebook Inc., undertaken under and in accordance with the Safe Harbour Privacy Principles and FAQs, is lawful, and remains lawful even where such data is accessed by national security authorities in the United States having regard to the express provision made in the Safe Harbour Privacy Principles and FAQs for third party access to the extent necessary to meet national security requirements.

7) The Respondent does not have jurisdiction to make a reference to the ECJ. Nor does the Respondent have jurisdiction to impugn or

invalidate domestic or EU law. In ***An Taoiseach v Information Commissioner*** [2011] 1 ILRM 508 a decision of the Information Commissioner was over-turned by the High Court because the Commissioner had taken it on herself to decide (a) that a set of regulations adopted in Ireland to transpose an EU Directive were deficient and (b) that she could dis-apply the regulations on the basis of her view. This is very close if not identical to what the Applicant wanted the Respondent to do in the present case. O'Neill J held that the consistency of domestic regulations with a Directive is something that can only be determined by a court of law. There were good reasons for reaching such a conclusion:

> *"The principle of legal certainty and clarity of laws in force would be undermined if national laws could not be enforced because of conflict with EU laws but were not lawfully repealed or declared invalid by a Court of competent jurisdiction. The principle of judicial protection would manifestly be breached if the rights and duties of parties to disputes concerning the application of EU laws could not be considered and determined by Courts established by law with competence to deal with these matters. The principle of proportionality would be at risk where the procedural route chosen to enforce EU law inflicted disproportionate damage on the national system of law and the rights and duties of the parties affected. The principle of subsidiarity would be ignored as the forum chosen might bear no resemblance to the appropriate forum for consideration and determination of the issue involved. The principle of equivalence would in effect be stood on its head. This principle requires that EU rights can be applied and enforced in national courts on no less favourable terms and conditions than similar actions arising under national law. The respondent's submission would result in EU rights enjoying a degree of procedural supremacy which not only far exceeds that available to similar actions based on national law, but virtually eliminates national procedural safeguards for rights and duties based on national law."* (page 532)

8) There is no doubt that data protection is a rapidly developing area of the law and, in particular, that there is an on-going and intensive debate taking place at an institutional level within the EU in relation to the capacity of the Safe Harbour Privacy Principles to provide adequate protection for the data privacy rights of citizens

of the European Union whose personal data is transferred to the United States. The manner in which the EU interacts with the United States in this context is clearly a matter that falls to be determined in the first instance by way of negotiations between the EU and the United States. Against that backdrop, and in the context of the development of specific legislative proposals for revisions to the existing regime, a Communication was issued by the European Commission on 27 November 2013, directed to the European Parliament and Council, in which the Commission recommended thirteen separate adjustments to the Safe Harbour Privacy Principles to address concerns raised about the operation of the Safe Harbour scheme in terms of transparency, availability of redress, enforcement, and access by US authorities to transferred data (**Exhibit "BH6"**). These recommendations remain the subject of discussion at EU level. They are also the subject of direct engagement between the EU and the United States in the context of ongoing dialogue between their respective justice and home affairs ministerial representatives.

9) So far as the subject matter of the Applicant's complaint is concerned, the Communication of 29 November 2013 contained recommendations under the heading "Access by US authorities", expressed in the following terms:

> *"12. Privacy policies of self-certified companies should include information on the extent to which US law allows public authorities to collect and process data transferred under the Safe Harbour. In particular companies should be encouraged to indicate in their privacy policies when they apply exceptions to the Principles to meet national security, public interest or law enforcement requirements.*
>
> *13. It is important that the national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly necessary or proportionate."*

10) On the same date, a report was published by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection ("**Exhibit MS2**" to the Applicant's Second Affidavit). Amongst other things, that report presents certain findings made by the EU co-chairs in connection with the legal basis on which surveillance

programmes are in fact carried out by US security agencies and the oversight and redress mechanisms to which they are subject.

11) For its part, the European Parliament has considered a report dated 8 January 2014, prepared by the Parliament's Committee on Civil Liberties, Justice and Home Affairs on "the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs")(**Exhibit "MS3"** to replying affidavit of the Applicant). On the basis of its consideration of that report, the Parliament adopted a resolution on 14 March 2014 in which (amongst other things) it called on the US authorities to put forward a proposal for a new framework for transfers of personal data from the EU to the US, to be substituted for the Safe Harbour framework, and which would meet EU law data protection requirements.

12) From the outset of dealing with the Applicant's complaint the Respondent emphasised the importance of the fact that the issues surrounding 'PRISM' are the subject of active and ongoing engagement at an EU level and at inter-governmental level. Thus in the Respondent's letter of reply dated 23 July 2103 (**Exhibit "MS10"**) he stated:

> *"We are aware of and welcome the fact that proportionality and oversight arrangements for programmes such as PRISM are to be the subject of high-level discussions between the EU and the USA."*

13) The Respondent also emphasised the fact that the Applicant had not established any basis for believing that any of his own personal data had been disclosed to US security authorities. Thus in the Respondent's letter of reply dated 25 July 2103 (**Exhibit "MS10"**) he stated:

> *"In making this assessment, the Commissioner is mindful of the fact that there is no evidence – and you have not asserted – that your personal data has been disclosed to the US authorities."*

14) By way of further illustration of the nature and extent of the on-going debate in this area, the documents that are adverted to in the affidavits and in the submissions of the Applicant include:

(i) Working Party Document on transfers of data to third countries (24 July 1998)(**Exhibit "MS6"**)

(ii) Working Party Document on SWIFT (22 November 2006)(**Exhibit "MS8"**)

(iii) Letter from Article 29 Data Protection Working Party to Vice President of the European Commission Viviane Reading (13 August 2013)(**Exhibit "MS16"**)

(iv) Speech of European Data Protection Supervisor to EU Parliament (7 October 2013)(**Exhibit "MS17"**)

(v) Communication from the European Commission to the Parliament and the Council (27 November 2013)(**Exhibit "BH6"**)

(vi) Report on the Findings by the EU Co-Chairs of the ad hoc EU-US Working Group on Data Protection (27 November 2013)(**Exhibit "MS2"** to the replying affidavit of the Applicant).

(vii) Draft Report of European Parliament Committee on Civil Liberties, Justice and Home Affairs (8 January 2014)(**Exhibit "MS3"** to replying affidavit of the Applicant)(subsequently adopted as a resolution of the European Parliament on 14 March 2014).

(viii) Article 29 Data Protection Working Party Document on surveillance of electronic communications for intelligence and national security purposes (10 April 2014).

(ix) Letter from Article 29 Data Working Party to Vice President of the European Commission Viviane Reading (10 April 2014).

Even this list does not capture the full extent of the exchanges that have taken place (and the reports delivered) in relation to the operation of the Safe Harbour framework.

15) Given these ongoing and substantial developments at EU and inter-governmental level (to which the Respondent is party in his capacity as a member of the Article 29 Working Group on Data Protection), we are a long way from ***N.S. v Secretary of State for***

the Home Department [2013] QB 102 where Member States were seeking to return asylum seekers to Greece even though they were fully aware that the Greek system had practically ground to a halt due to the fact that almost 90% of all illegal immigrants entering the EU in 2010 came into Greece (see para 87 of the decision). As set out above, in the present case, the Respondent expressly noted the fact that proportionality and oversight arrangements for security programmes impacting on the data privacy rights of citizens are the subject of ongoing high-level discussions between the EU and the United States.

16) In his assessment of a similar complaint made by the Applicant concerning data transfers by Skype and Microsoft, the Luxembourg Data Protection Commissioner appears to have taken the same approach, concluding that the Commission Decision authorises the transfer of personal data from the European Economic Area to the United States and, further, that he cannot make a reference to the ECJ (**Exhibit "MS1"** to the replying affidavit of the Applicant).

17) It is submitted that in forming the impugned opinion, the Respondent acted within jurisdiction and that it follows that the Applicant is not entitled to relief by way of judicial review.

18) It is important to note that the forming of an opinion not to investigate a complaint at a particular point in time is not necessarily a final one for all time and nor does it preclude a fresh complaint being made if the law changes or if further evidence becomes available. For example, if the Commission Decision were to be revoked and/or replaced at some future date then clearly any new complaint that the Applicant might wish to bring would fall to be considered under the new legal regime in place. However the Respondent has to have regard to the state of the law as it stands as at the time when he is considering a particular complaint. That is what was done in this case.

19) It is relevant to note that a decision not to investigate a complaint on the basis that it is frivolous or vexatious is clearly a discretionary decision. The courts are slow to second-guess discretionary decisions by way of judicial review. In ***Killiea v Information Commissioner*** [2003] 2 IR 402 the applicant challenged a decision of the Information Commissioner to

discontinue an investigation. The High Court declined to intervene. Murphy J stated that:

> *"The reason for his decision to discontinue the review is set out in his letter of the 11th March, 2002. There is nothing in that letter which would suggest that the Commissioner was acting outside of the powers conferred upon him by the Act."* (para 8.2)

Murphy J continued:

> *"If a decision of the Commissioner to discontinue a review, taken in the exercise of the discretion vested in him by the Oireachtas by means of section 34 (9) of the Act is, properly speaking, within the scope of section 42 (1) of the Act, the Court ought only to upset the Commissioner's exercise of such discretion if the same were found to have fallen foul of the judicial review standard of reasonableness. In other words, the Court ought not to interfere with the Commissioner's decision to discontinue his review of the decision made by the Department in this case unless it considers his decision to fly in the face of fundamental reason or common sense or to be so irrational or unreasonable that no reasonable Commissioner could have come to it."* (para 8.3)

20) Finally it may be noted that the recent decision of the ECJ in ***Digital Rights Ireland v Minister for Communications, Marine and Natural Resources*** [2014] EUECJ C-293/12, (unreported, Grand Chamber, 8th April 2014) was a case where the High Court in Ireland had been asked in plenary proceedings brought against the State to declare the invalidity of Directive 2006/24 and of Part 7 of the Criminal Justice (Terrorist Offences) Act 2005. The High Court in Ireland had made a reference to the ECJ to determine the validity of the Directive. Clearly it cannot be suggested that the Respondent in this case had jurisdiction to declare any Irish or EU law to be invalid. The ECJ concluded that the Directive was invalid and stated:

> *"… 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 …" (para 54)

This is obviously a ruling that the Member States will have to pay regard to if they decide to amend the Commission Decision and to adjust the Safe Harbour Privacy Principles and FAQs previously agreed with the United States.

B) The legal framework.

Domestic law

21) Section 10(1) of the DP Acts provides that:

(a) The Commissioner may investigate, or cause to be investigated, whether any of the provisions of this Act have been, are being or are likely to be contravened in relation to an individual either where the individual complains to him of a contravention of any of those provisions or he is otherwise of opinion that there may be such a contravention.

(b) Where a complaint is made to the Commissioner under paragraph (a) of this subsection, the Commissioner shall-

(i) investigate the complaint or cause it to be investigated, unless he is of opinion that it is frivolous or vexatious, and,

(ii) if he or she is unable to arrange, within a reasonable time, for the amicable resolution by the parties concerned of the matter the subject of the complaint, notify in writing the individual who made the complaint of his or her decision in relation to it and that the individual may, if aggrieved by the decision, appeal against it to the Court under section 26 of this Act within 21 days from the receipt by him or her of the notification.

22) In this case the Commissioner formed the opinion that the

complaint was frivolous or vexatious.

23) Section 11 of the DP Acts addresses the issue of the transfer of personal data outside of the State.

24) Section 11(2)(a), which was inserted by the 2003 Act, provides that:

> (a) Where in any proceedings under this Act a question arises-
>
> (i) whether the adequate level of protection specified in subsection (1) of this section is ensured by a country or territory outside the European Economic Area to which personal data are to be transferred, and
>
> (ii) a Community finding has been made in relation to transfers of the kind in question,
>
> the question shall be determined in accordance with that finding.

25) Section 11(2)(b) of the DP Acts defines the concept of a Community finding in the following terms:

> In paragraph (*a*) of this subsection 'Community finding' means a finding of the European Commission made for the purposes of paragraph (4) or (6) of Article 25 of the Directive under the procedure provided for in Article 31(2) of the Directive in relation to whether the adequate level of protection specified in subsection (1) of this section is ensured by a country or territory outside the European Economic Area.

26) The Commission Decision is made pursuant to Article 25(6) of Directive 95/46/EC and so comes within the definition of a 'Community finding'.

27) It is submitted that Section 11(2) makes it clear that where matters relating to international data transfer out of the EU have been dealt with at an EU level then it is not for domestic regulators to seek to go behind that. One can readily see the logic of this since

it would be very difficult for the EU to trade with the US if every member state took a different approach to this issue. It is the type of issue that is much more appropriately dealt with at an inter-governmental level.

EU law

28) The DP Acts were enacted to give effect to the Data Protection Convention 1981 and Directive 95/46/EC ("the Directive"). Article 16 of the Lisbon Treaty also makes express reference to the need to protect personal data and provides that "Everyone has the right to protection of personal data concerning him or her."

29) In respect of some countries (such as Argentina, Canada, Israel and Switzerland) the EU has issued individual decisions recognising them as providing adequate protection for personal data on the basis that those countries have generally applicable data protection law which follows the approach of the Directive.

30) The Commission Decision was adopted to establish the Safe Harbour Principles and FAQs as a reference point for permissible data transfers to the US on the basis that the US has a very different approach to data protection than the EU (being based on piece-meal legislation, self-regulation and consumer action) and there was a concern that personal data would stop flowing to the US after the implementation of the Directive in the EU.[1] The Safe Harbour Privacy Principles and FAQs were issued by the US Department of Commerce on 21 July 2000 and, following the adoption of the Commission Decision on 26 July 2000, they came into effect in November 2000.

31) The Commission Decision is thus the relevant 'Community finding' that governs this area of the law. The Safe Harbour Privacy Principles and FAQs are contained in the Annexes to the Commission Decision. The FAQs amplify the principles and deal with certain practical points relating to the application of the Safe Harbour Privacy Principles.

32) Participation in the Safe Harbour framework is voluntary for any particular organisation. Where an organisation elects to

[1] See generally Jay, *Data Protection Law and Practice* (Sweet and Maxwell, 4th ed. 2012), Chapter 8

participate, however, it is required to certify to the US Department of Commerce that it is operating in compliance with the Safe Harbour Privacy Principles. Amongst other things, it must adopt a publicly stated privacy policy incorporating the standards set out in the Principles and the FAQs. Upon so certifying, the Principles and FAQs become legally binding on the organisation in question and they may be enforced against it. Certification lasts for a period of 12 months. The organisation must make an annual return to the Department confirming its continued compliance.

33) Amongst other things, participants are required to adopt effective and independent complaints and dispute resolution procedures. Separately, and depending on the particular sector in which they are operate, they must subject themselves to regulation by the Federal Trade Commission or the US Department of Transportation.

34) The US Department of Commerce maintains a publicly accessible list of participants in the Safe Harbour scheme. Amongst other things, the listing identifies the enforcement and independent dispute resolution agency applicable to each participant.

35) Failure to comply with the Safe Harbour Privacy Principles and FAQs in the US can result in an organisation being the subject of enforcement proceedings by the Federal Trade Commission. In the context of such proceedings, the Commission may impose significant financial penalties. It may also direct the strike-off of an organisation from the above-referred list, causing the organisation to lose its Safe Harbour status.

36) Recital 9 of the Commission Decision expressly recognises that it may need to be reviewed by the EU in the light of experience:

> *"The 'safe harbor' created by the Principles and the FAQs, may need to be reviewed in the light of experience, of developments concerning the protection of privacy in circumstances in which technology is constantly making easier the transfer and processing of personal data and in the light of reports on implementation by enforcement authorities involved."*

This is precisely what is currently happening.

37) Article 4 of the Commission Decision provides:

> *"This Decision may be adapted at any time in the light of experience with its implementation and/or if the level of protection provided by the Principles and the FAQs is overtaken by the requirements of US legislation."*

38) Obviously any such reviews and/or adaptations will occur at an EU and/or EU-US level. It is not for the Respondent to pre-empt what the outcome of the current debate may be.

39) The Safe Harbour Principles set out at Annex 1 of the Commission Decision expressly state that:

> *"adherence to these principles may be limited (a) to the extent necessary to meet national security, public interest or law enforcement requirements …."* .

40) The preamble to the Principles contained at Annex 1 of the Commission Decision expressly states that:

> *"US law will apply to questions of interpretation and compliance with the Safe Harbour Principles (including the Frequently Asked Questions) and relevant privacy policies by safe harbour organisations, except where organisations have committed to cooperate with European Data Protection Authorities ..."* .

41) Under Article 3 of the Commission Decision, a national Data Protection Authority can direct the suspension of data flows to an entity that has self-certified its adherence to the safe harbour principles in two specific scenarios:

a. Where a relevant US enforcement authority has determined that the receiving entity is violating the safe harbour principles; or,

b. Where the following circumstances arise:

    i. There is a substantial likelihood that the Principles are being violated;

ii. There is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue;

iii. The continuing transfer would create an imminent risk of grave harm to data subjects; and,

iv. The competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond.

42) It is clear that (a) has no application here. So far as (b) is concerned, the position is as follows.

43) No evidence was put before the Commissioner by the Applicant on which the Commissioner could possibly have concluded that there was a *substantial* likelihood that the Safe Harbour Principles were in fact being violated in the case of data transfers between Facebook Ireland Limited and Facebook Inc. On the contrary, the Applicant's complaint was essentially speculative in nature. Nor did the Applicant adduce any evidence to suggest that there was an imminent risk of grave harm to him, or that any of *his* data had been or was likely to be accessed by the NSA.

44) Equally, the Applicant put forward no factual or other material on which the Commissioner could reasonably have concluded that the enforcement mechanisms provided for under the Safe Harbour Privacy Principles were not addressing (and would not address) the issues raised insofar as they affected the Applicant and that the relevant enforcement and/or dispute resolution agency would not "take adequate and timely steps to settle the case at issue". It appears that the Applicant did not seek to have recourse to the enforcement mechanisms provided for under the Safe Harbour Privacy Principles.

45) Nor is it clear how the Commissioner could himself have investigated or determined whether, for example, the NSA was being afforded access to Facebook subscriber data in a way, or to an extent, that was not consistent with the Safe Harbour Privacy Principles and/or national or European data protection law. As noted at paragraphs 15, 23 and 25 of his First Affidavit, the

Commissioner was in fact informed by Facebook Ireland Limited (being the transferring party) that the media reports on which the Applicant grounded his complaint (being reports to the effect that the NSA was in a position to obtain direct and unhindered access to bulk data held on servers located in the US relating to Facebook subscribers) were not correct.

46) Against this backdrop, and in circumstances where the EU Commission was already engaged in a substantial review of the operation of the Safe Harbour scheme with a view to effecting material changes to that scheme, it was perfectly lawful and rational for the Commissioner to take the view that the Applicant's complaint should properly be addressed at EU level and not by him.

The nature of the Respondent

47) It may be relevant to some of the issues that arise in this judicial review to make some observations on the legal nature of the Respondent. The Respondent has jurisdiction to make decisions in respect of complaints. Unlike the Financial Services Ombudsman, the Respondent cannot award damages to a complainant. Unlike the position as regards a Finding of the Financial Services Ombudsman, the fact that a complaint has been made to the Respondent does not preclude a member of the public from litigating a grievance against someone who he believes has misused his data. By way of example Section 7 of the DP Acts provides that:

> "For the purposes of the law of torts and to the extent that that law does not so provide, a person, being a data controller or a data processor, shall, so far as regards the collection by him of personal data or information intended for inclusion in such data or his dealing with such data, owe a duty of care to the data subject concerned…".

C) The basic principles of judicial review.

48) As this is a judicial review it is the Applicant who bears the burden of proof in terms of establishing that he is entitled to the reliefs sought.[2]

[2]In Collins and O'Reilly, Civil Proceedings and the State, the principle is explained in the following terms: "*The [cross-examination] procedure is of assistance where the affidavits, on their face, disclose*

49) In ***Nowak v Data Protection Commissioner*** [2013] 1 ILRM 207 Birmingham J set down the standard of review of a decision of the Commissioner in the following terms:

> *"I am satisfied that the approach identified by Finnegan P. is the one that it would have been appropriate to apply had an appeal been available. In particular it seems to me that it would have been appropriate for the court to have regard to what Finnegan P. referred to as the deferential standard, when deciding to substitute its own view for that of the Data Protection Commissioner on the issue of whether an exam script constituted personal data. The Data Protection Commissioner is concerned with issues involving data protection on a daily basis. He is required to be in regular contact with his colleagues in other EU Member States and is likely to be fully au fait with development internationally. Pointing to the expertise of the Data Protection commissioner does not mean that a court will abdicate its responsibilities and there may be cases where decisions of the Commissioner will be set aside, but if that happens, the decision to set aside the decision will have been taken by a court that is conscious of the experience and expertise of the Commissioner."* (page 214)

Whilst the above comments were made in the context of a statutory appeal, there is no reason why the principle of deference would be any different in a judicial review.

50) The comments of Finnegan P that were being followed by Birmingham J come from ***Ulster Bank v Financial Services Ombudsman*** [2006] IEHC 323, where Finnegan P (as he then was) laid down the following test for an appeal from the Financial Services Ombudsman:

> *"In short, the appeal provided for under this legislation was not intended to take the form of a re-examination from the beginning of the merits of the decision appealed from culminating, it may be, in the substitution by the High Court of its adjudication for that of the first defendant. It is accepted that, at the other end of the spectrum, the High*

---

conflicts of fact that are incapable of resolution. The court cannot resolve such conflicts in favour of the party on whom the burden of proof lies, usually the applicant." (para 5-86)

Court is not solely confined to the issues which might arise if the decision of the first defendant was being challenged by way of judicial review. In the case of this legislation at least, an applicant will succeed in having the decision appealed from set aside here (sic) it establishes to the High Court as a matter of probability that, taking the adjudicative process as a whole, the decision reached was vitiated by a serious and significant error or a series of such errors. In arriving at a conclusion on that issue, the High Court will necessarily have regard to the degree of expertise and specialised knowledge available to the [first defendant]."

51) In fact a judicial review is even narrower than a statutory appeal in respect of the extent to which the Court will engage review the merits of the decision that has been made.

52) In a well-known passage in ***Associated Picture House v Wednesbury*** [1948] 1 KB 223 Lord Greene MR set out the test for challenging administrative decisions:

"The Court is entitled to investigate the action of the [authority] with a view to seeing whether they have taken into account matters which they ought not to take into account or, conversely, have refused to take into account or neglected to take into account matters which they ought to take into account. Once that question is answered in favour of the [authority], it may still be possible to say that, although the [authority] have kept within the four corners of the matters which they ought to consider, they have nevertheless come to a conclusion so unreasonable that no reasonable [authority] could ever have come to it. In such a case, again, I think the Court can interfere. The power of the Court to interfere in each case is not as an appellate authority to override a decision of the [authority], but as a judicial authority which is concerned only, to see whether the [authorities] have contravened the law by acting in excess."

53) Morris P reflected on the function of judicial review in his decision in ***Bailey v Flood***, unreported, 6 March 2000 where he stated:

"The function of the High Court on an application for

judicial review is limited to determining whether or not the impugned decision was legal, not whether or not it was correct. The freedom to exercise a discretion necessarily entails the freedom to get it wrong; this does not make the decision unlawful. Consideration of the alternative position can only confirm this view. The effective administration of a tribunal of inquiry would be impossible if it were compelled at every turn to justify its actions to the High Court."

54) In ***Henry Denny & Sons v Minister for Social Welfare***, [1998] 1 IR 34 at 37-38, Hamilton CJ stated that:

"…I believe it would be desirable to take this opportunity of expressing the view that the Courts should be slow to interfere with the decisions of expert administrative tribunals. Where conclusions are based upon an identifiable error of law or an unsustainable finding of fact by a tribunal such conclusions must be corrected. Otherwise it should be recognised that tribunals which have been given statutory tasks to perform and exercise their functions, as is now usually the case, with a high degree of expertise and provide coherent and balanced judgments on the evidence and arguments heard by them it should not be necessary for the Courts to review their decisions by way of appeal or judicial review."

55) In ***ACT Shipping v Minister for the Marine*****,** [1995] 3 IR 406 at 431, Barr J stressed that the Court should be loathe to interfere with *intra vires* administrative decisions.

D) The basis for the impugned opinion.

56) The Respondent formed his opinion on the basis of Section 11 of the DP Acts, the Commission Decision, the terms of the Safe Harbour Privacy Principles and FAQs, Facebook Incorporated's certificate of adherence to the Safe Harbour Principles and FAQs, and on the fact that the difficult issues that arise in connection with the nature and extent of the access afforded to national security agencies in the US to transferred data are currently being examined and dealt with at an EU-US level with a view to agreeing material changes to the Safe Harbour scheme as presently constituted.

57) On a number of alternative bases, most notably on the basis of the operation of the Safe Harbour Privacy Principles, the transfer of subscriber data to the United States is permissible under national and EU data protection law.

58) The Safe Harbour Principles, as endorsed by the European Union by means of the Commission Decision, expressly permit (subject to certain limited constraints) the accessing of personal or subscriber data where necessary to meet national security, public interest or law enforcement requirements.

59) It is clear that the Applicant is dissatisfied with the Commission Decision and believes that, as a matter of principle, the Safe Harbour framework it establishes does not provide sufficient protection for the data privacy rights of citizens whose data is transferred to the United States. Thus one of his grounds of challenge in the judicial review is that the Respondent was compelled to conclude that the Commission Decision "*can no longer represent good law"* whether by reference to the passage of time or by reference to what the Applicant refers to as *"higher ranking law"*. It is the right of the Applicant to disagree with the Commission Decision. However it is not a matter that the Commissioner can provide a remedy in respect of.

60) The Respondent concluded that, in effect, what the complaint demanded of him was that he should agree to set aside or disapply the Commission Decision in circumstances where, under the express terms of Section 11(2) of the DP Acts, the Respondent is statutorily bound to apply it. Against this backdrop, and having regard to the terms of the Safe Harbour Privacy Principles, and the certificate held by Facebook Incorporated confirming compliance with those principles, the Respondent considered that he would have no standing to address the substance of the Applicant's complaint and that the complaint was one that could only properly be addressed by the relevant institutions of the European Union.

61) In addition the Respondent has no jurisdiction to accede to the Applicant's request that he make a reference to the ECJ.

62) The fact that other data protection commissioners in other EU states may be dealing with complaints that the Applicant (or anyone else) has made to them in a particular way is not a recognised legal basis for asserting that an opinion formed by the

Respondent is thereby irrational and/or unreasonable. The Respondent is obliged to form his own opinion on a particular complaint submitted to him and if he were to regard himself as bound by the approach of other data protection authorities that would amount to a fettering of his discretion. In any event it does not appear that the Applicant has secured a different outcome in any other jurisdiction where he has complained.

63) The Respondent also noted that the Applicant did not appear to allege that *his* subscriber data had in fact been transferred to the United States and accessed by a U.S. national security authority. Rather, his complaint was framed in general terms, and appeared to be made in some sort of representative capacity on behalf of Facebook subscribers' generally, or a group of Facebook subscribers. The Applicant is only entitled to rely on the precise facts and circumstances of his own case and is not entitled to rely on a *jus tertii.* In the words of Hardiman J in ***A v Governor of Arbour Hill Prison*** [2006] 4 IR 88 at 165:

> *"… a person who seeks to invalidate a statutory provision must do so by reference to the effect of the provision on his own rights. He cannot seek to attack the section on a general or hypothetical basis and specifically may not rely on its effect on the rights of a third party: see Cahill v Sutton [1980] IR 269. In other words, he is confined to the actual facts of this case and cannot make up others which would suit him better."*

64) In his written submissions the Applicant appears to suggest that under Article 3(b) of the Commission Decision, the Respondent should at the very least have sought clarification from Facebook Ireland Limited as to the veracity or otherwise of allegations that Facebook Incorporated's servers in the US had been accessed on "bulk basis" by a US security agency. The implicit criticism appears to be that the Respondent did nothing more than check to see that Facebook Inc. had a Safe Harbour certificate in place. The following points arise in respect of this suggestion.

65) It is not accurate to say that Article 3(b) of the Commission Decision compelled the Respondent to reach a different opinion and compelled him to investigate this particular complaint from the Applicant.

66) Firstly, as referenced at paragraph 15 of the Respondent's first affidavit, the 'PRISM' allegations were the subject of discussion between the Respondent and Facebook Ireland Limited before he had received the Applicant's complaint. In the course of those discussions, Facebook Ireland Limited confirmed that its US parent does not provide access to US security agencies to subscriber data save by means of targeted requests, properly and lawfully made. The position as set out by Facebook Ireland Limited was accepted by the Respondent because he was aware, on the basis of an audit that had been carried out by his office of Facebook's operations in Ireland (details of which are the subject of two publicly available reports), that Facebook had appropriate procedures in place for the handling of access requests received from security agencies generally.

67) Secondly, the Applicant did not establish any basis for believing that *his* personal data had been accessed by the NSA. In fact, on its terms, the complaint did not even appear to assert that the Applicant's personal data had been so accessed.

68) Thirdly, no evidence was put before the Respondent by reference to which he could have assessed the Applicant's complaint on its merits. The complaint was essentially speculative, in that the Applicant simply demanded that the Respondent accept, as an established fact, the contention that Facebook Inc. had indeed provided direct and unhindered access to bulk subscriber data held on its servers to a particular US security agency.

69) Finally it is submitted that for the Respondent to rely on the law as expressed in the Commission Decision does not amount to a fettering of his discretion. As a statutory decision-maker the Respondent is obliged to have regard to the relevant law.

E) The challenge to the merits of the impugned opinion.

70) Several of the Applicant's grounds of challenge relate to the merits of the impugned opinion and may be conveniently addressed together. These include claims that the impugned opinion is irrational, is based on a misinterpretation of the DP Acts, is based on matters that were irrelevant to the complaint etc. The basis for the impugned opinion has already been set out above and will not be repeated here. It is submitted that the issue is not whether or not this Court agrees with the Respondent's opinion or would have

formed the same opinion itself. Rather the issue is whether or not the impugned opinion is one that was made within jurisdiction and is rational and lawful. It is submitted that the answer to all of these questions is yes.

71) As set out above, the standard of review for decisions and opinions of the DPC has been established by ***Nowak*** where Bermingham J stated that:

> *"…it seems to me that it would have been appropriate for the court to have regard to what Finnegan P referred to as the deferential standard, when deciding to substitute its own view for that of the Data Protection Commissioner on the issue of whether an exam script constituted personal data."*

72) The test for irrationality was set down in ***Associated Picture House v Wednesbury*** [1948] 1 KB 223. In ***O'Keeffe v. An Bord Pleanala*** [1993] 1 IR 39 the Supreme Court held that the onus lay on the applicant seeking judicial review to establish that the respondent board had no relevant material before it to support its decision. In judicial review proceedings, the Court will not substitute its own view for that of the decision-maker sought to be reviewed. If there was any relevant material before the decision-maker to support its decision, the Court will not interfere.

73) The plea of *ultra vires* does not appear to add anything to the plea of irrationality in the context in which it is made. In ***Kenny v Judge Coughlan*** [2008] IEHC 28 O'Neill J. rejected a challenge to a speeding offence conviction. The applicant argued that the prosecution had failed to adduce sufficient evidence of his speed and raised various complaints about the evidence adduced against him. O'Neill J. rejected these complaints and stated that *"Even if the respondent erred in this regard (and there is no indication that he did), that error would clearly have been an error within jurisdiction and not amenable to the remedy of judicial review."*

F) The challenge to the procedures adopted.

74) It appears that some of the grounds of challenge may be procedural in nature, although this does not appear to be at the forefront of the Applicant's challenge.

75) In the first place it is submitted that, as he had done in the

case of twenty-two other complaints submitted by the Applicant (each of which is being addressed on its merits), the Respondent carried out a sufficient level of examination so as to determine in the first instance whether or not the complaint disclosed a discernable data protection issue requiring investigation or, alternatively, whether the complaint was frivolous or vexatious. As Section 10(1)(b)(i) of the DP Acts makes it clear that the forming of an opinion that a complaint is frivolous or vexatious is an alternative to investigating a complaint, it follows that an investigation is not itself required prior to forming an opinion not to hold an investigation.

76) In so far as the Applicant alleges that the opinion formed by the Respondent was formed in breach of the Applicant's fundamental right to be heard, it is submitted that the Applicant was given every opportunity to make his complaint.

77) At no stage during the impugned process did the Applicant seek any further right to be heard. In the circumstances the Applicant is estopped and/or is guilty of acquiescence in respect of this issue and so cannot complain about it now.

78) In terms of any complaint as to reasons it should be noted that the Commissioner is not delivering a judgment in the manner in which a court of law would deliver a judgment. In ***Faulkner v Minister for Industry and Commerce*** [1997] ELR 107 at 111 O'Flaherty J stated, in a classic exposition of the law, that:

> *"[W]hen reasons are required from administrative tribunals they should be required to give only the broad gist of the basis of their decisions. We do no service to the public in general, or to particular individuals, if we subject every decision of every administrative tribunal to minute analysis."*

79) In ***Kenny v Judge Coughlan*** [2008] IEHC 28 O'Neill J stated that "*In my opinion it is not necessary for a District Judge to give analytical reasons for the acceptance or rejection of any particular piece of evidence. It is sufficient to merely indicate an acceptance or rejection of the evidence offered on either side of the case."* This was followed by Kearns P in ***Sisk v Judge O'Neill*** [2010] IEHC 96. In ***Lyndon v Judge Collins*** [2007] IEHC 487 Charleton J stated that *"What is essential, however, is that people*

know going out of any District Criminal Court what they have been convicted for and why they have been convicted, and in this case I think that it is clearly implied in what the learned District Judge said that she was convicting the accused because of the fact that she completely rejected his testimony and accepted instead the testimony of the prosecution."

80) It is the case that in ***EMI Records (Ireland) Ltd v The Data Protection Commissioner*** [2013] IESC 34, [2014] 1 ILRM 225, a decision of the Respondent was quashed. That was a case where there had been an investigation by the Respondent and where the Supreme Court held that no reasons at all had been given for the decision to uphold the complaint in question.

81) It is submitted that the right to good administration as protected by Article 41 of the Charter and as applied in cases such as ***M.M. v Attorney General*** [2012] EUECJ C-277/11; [2013] 1 WLR 1259, does not add anything that is not already recognised by our domestic principles of fair procedures and natural justice.

G) The EU and the Convention

82) It is submitted that the Applicant's invocation of EU and Convention rights do not add anything to his challenge to the merits of the impugned opinion. The DP Acts are the domestic implementation of the State's EU obligations in this area and also protect the relevant Convention rights. Thus if the Commissioner has acted within jurisdiction under the DP Acts it is unclear how any stand-alone EU or Convention case arises on the facts of this particular case.

83) In respect of the allegation that the impugned opinion is in breach of EU law, it is submitted that this cannot be the case since the impugned opinion was based on EU law, namely the Commission Decision.

84) Equally, no stand-alone claim under the European Convention on Human Rights arises. The Convention does not form part of the domestic law of the State. The Applicant has not sought or obtained leave to seek any relief pursuant to the European Convention on Human Rights Act, 2003.

85) In any event it is not the case that the Applicant's right to a fair trial under Article 6 of the Convention was breached by the impugned opinion. None of the civil rights or obligations of the Applicant were determined by the impugned opinion. In particular the Applicant did not submit any evidence that his own data had been accessed by the NSA. Without prejudice to that, the entire scheme of the DP Acts together with the availability of judicial review amounts to compliance with Article 6.

86) Nor is the Applicant's right to respect for his private and family life under Article 8 of the Convention breached by the impugned opinion. In particular the Applicant did not submit any evidence that his own data had been accessed by the NSA.

87) It is submitted that there is nothing in cases such as ***Osterreichischer Rundfunk*** [2003] EUECJ C-138/01 (20 May 2003) that is inconsistent with the above.

H) Relying on new material/estoppel and acquiescence.

88) It is submitted that the Applicant is only entitled to rely on the material that he submitted to the Respondent as part of his complaint and cannot seek to challenge the impugned opinion by reference to material that he did not submit to the Respondent.

89) In ***Rotunda Hospital v Information Commissioner*** [2011] IESC 26 Fennelly J held that,

> "*I think it is an integral part of any appeal process, other than possibly an appeal by complete re-hearing, that any point of law advanced on appeal shall have been advanced, argued and determined at first instance"* (para 35).

Macken J added that,

> "*…the general law requires that a party will bring forward, at least in the context of legal proceedings, his entire case, so that there is no incremental decision making process, and by analogy it seems to me appropriate to find that, save in some exceptional circumstance, which does not appear to arise here, the hospital was obliged to bring forward before the Commissioner, all points of law upon which it wished to rely…"*

That case concerned an appeal on a point of law but it is submitted that the same principle applies.

I) Conclusion.

90) Judicial review is a discretionary remedy. This was made clear by Denham J in ***De Roiste v Minister for Defence*** [2001] 1 IR 190 at 204 who stated:

> *"Judicial review is an important legal remedy, developed to review decision-making in the public law domain. As the arena of public law decision-making has expanded so too has the volume of judicial review. It is a great remedy modernized by the Rules of the Superior Courts, 1986, and by precedent. However, there is no absolute right to its use, there are limitations to its application. The granting of leave to apply for judicial review and the determination to grant judicial review are discretionary decisions for the court. This has been set out clearly in precedent."*

91) In the present case it is submitted that the Court should exercise its discretion not to grant relief. It is clear that this area is evolving in a rapid manner at an international political level and that this is the level at which the Applicant's concerns are more properly addressed.

Paul Anthony McDermott
26 April 2014