High Court of Ireland Decisions

Judgment Title: Schrems -v- Data Protection Commissioner

Neutral Citation: [2014] IEHC 310

High Court Record Number: 2013 765 JR

Date of Delivery: 18/06/2014

Court: High Court

Composition of Court:

Judgment by: Hogan J.

Status of Judgment: Approved

Neutral Citation Number: [2014] IEHC 310

THE HIGH COURT

[2013 No. 765JR]

BETWEEN/

MAXIMILLIAN SCHREMS

APPLICANT

AND

DATA PROTECTION COMMISSIONER

RESPONDENTS

JUDGMENT of Mr. Justice Hogan delivered on the 18th June, 2014

I

1. In May, 2013 a computer systems administrator named Edward Snowden - who up to that point had been working for the international consulting firm Booz Allen Hamilton - caused a sensation following his arrival in Hong Kong. Mr. Snowden's firm had been contracted to work for the US National Security Agency ("NSA"). In the course of that employment Mr. Snowden unlawfully appropriated thousands of highly classified NSA files which, when disclosed by him following his arrival in Hong Kong to media outlets such as *The Guardian* (in the UK) and the *New York Times* and the *Washington Post* (in the US), revealed the interception and surveillance of internet and telecommunications systems by the NSA on a massive, global scale.

2. These revelations form the backdrop to the present judicial review application. The applicant, Mr. Schrems, maintains that as the Snowden disclosures demonstrate that there is no effective data protection regime in the United States, the respondent Data Protection Commissioner ("the Commissioner") should exercise his statutory powers to direct that the transfer of personal data from Facebook Ireland to its parent company in the United States should cease. The Commissioner for his part maintains that he is bound by the terms of a finding of the European Commission in July 2000 to hold that the data protection regime in the United States is adequate and effective where the companies which transfer or process the data to the United States self-certify that they comply with the principles set down in this Commission decision. The European Commission decision of July 2000 sets up a regime known as the Safe Harbour regime and one of the many issues which arise from these proceedings is whether the Safe Harbour principles are still effective and functional some fourteen years after that decision and finding.

3. Central to the entire case is the Commissioner's conclusion that the applicant's complaint is unsustainable in law, precisely because the Safe Harbour regime gives the *imprimatur* to such data transfers on the basis that the European Commission concluded that the US does, in fact, provide for adequate data protection. The applicant maintains in turn that this decision of the Commissioner is unlawful.

II

4. While it is true that the Snowden disclosures caused - and are still causing - a sensation, only the naïve or the credulous could really have been greatly surprised. The question of transnational data protection and state surveillance is admittedly difficult and sensitive and, subject to fundamental legal protections, a satisfactory *via media* can in many respects be resolved only at the level of international diplomacy and *realpolitik*. While a court must naturally be aware of these underlying realities, in resolving issues such as arise in the present case it must nonetheless endeavour to apply neutrally the applicable legal materials.

5. Yet only the foolish would deny that the United States has, by virtue of its superpower status, either assumed - or, if you prefer, has had cast upon it - far-reaching global security responsibilities. It is probably the only the world power with a global reach which can effectively monitor the activities of rogue states, advanced terrorist groups and major organised crime, even if the support of allied states such as the United Kingdom is also of great assistance in the discharge of these tasks and responsibilities. The monitoring of global communications - subject, of course, to key safeguards - is accordingly regarded essential if the US is to discharge the mandate which it has thus assumed. These

surveillance programmes have undoubtedly saved many lives and have helped to ensure a high level of security, both throughout the Western world and elsewhere. But there may also be a suspicion in some quarters that this type of surveillance has had collateral objects and effects, including the preservation and re-inforcing of American global political and economic power.

6. One may likewise fairly assume that the Snowden revelations have compromised these important national security programmes. This will certainly hamper entirely legitimate counter-terrorism operations and, by reason of the possibly inadvertent disclosure of personal information, perhaps even the lives of security operatives working overseas have been put at risk: see *Miranda v. Home Secretary* [2014] EWHC Admin 255 where these adverse effects of the Snowden revelations were summarised by Laws L.J. for the English High Court in these terms by reference to evidence tendered in that case by security specialists and operatives.

7. It would, however, be equally naïve to believe that this sort of surveillance is the preserve of the superpowers. One may fairly assume that even those states - both big and small - who protested loudly in the wake of the Snowden revelations concerning the invasion of the data protection of their citizens would not themselves be above resorting to such irregular espionage (*i.e.*, surveillance and interception of communications which are not provided for by law) where it suited their interests. This might be especially so where these governments could conveniently turn a blind eye to such surveillance and interception activities on the part of their security forces, or, better still, where they could credibly deny that such espionage had ever been officially "sanctioned."

8. On the other hand, the Snowden revelations demonstrate a massive overreach on the part of the security authorities, with an almost studied indifference to the privacy interests of ordinary citizens. Their data protection rights have been seriously compromised by mass and largely unsupervised surveillance programmes.

9. It is necessary now to say something briefly about the PRISM programme, the details of which were at the core of the Snowden revelations.

III

The Snowden revelations and the PRISM programme

10. According to a report in *The Washington Post* published on 6th June 2013, the NSA and the Federal Bureau of Investigation ("FBI"):

> "are tapping directly into the central servers of nine leading US internet companies, extracting audio and video chats, photographs, e-mails, documents and connection logs that enable analysts to track foreign targets…."

11. According to the *Washington Post* the programme is code-named PRISM and it apparently enables the NSA to collect personal data such as emails, photographs and videos from major internet providers such Microsoft, Google and Facebook. This is done on a mass scale in accordance with orders made by the US Federal Intelligence Court sanctioning such activities.

12. In a report in *The Guardian* newspaper dated 31st July, 2013, it was claimed that a top secret NSA programme entitled "X Keyscore" enabled it to collect "nearly everything a user does on the internet". The report further claimed that:

> "A top secret NSA programme allows analysts to search with no prior authorisation through vast databases containing emails, online chats and the browsing history of millions of individuals, according to documents provided by whistleblower Edward Snowden."

13. While there may be some dispute regarding the scope and extent of some of these programmes, it would nonetheless appear from the extensive exhibits contained in the affidavits filed in these proceedings that the accuracy of much of the Snowden revelations does not appear to be in dispute. The denials from official sources, such as they have been, were feeble and largely formulaic, often couched in carefully crafted and suitably ambiguous language designed to avoid giving diplomatic offence. I will therefore proceed on the basis that personal data transferred by companies such as Facebook Ireland to its parent company in the United States is thereafter capable of being accessed by the NSA in the course of a mass and indiscriminate surveillance of such data. Indeed, in the wake of the Snowden revelations, the available evidence presently admits of no other realistic conclusion.

IV

14. It is, however, appropriate to note that many of the activities of the NSA are subject to the supervision of the Foreign Intelligence Surveillance Court as provided for by the US federal statute, the Foreign Intelligence Surveillance Act 1978 ("the FISA Court"). The FISA Court is a specialist court consisting of federal judges enjoying standard constitutional guarantees in relation to tenure and independence. This Court entertains applications by the NSA for warrants in relation to foreign surveillance and interception of communications.

15. It would seem, however, that the FISA Court's hearing are entirely conducted in secret, so that even the court orders and its jurisprudence remain a closed book. The US security authorities are, in effect, the only parties who are or who can be heard in respect of such applications before the FISA Court. One of the striking features of the Snowden revelations was the disclosure of (hitherto secret) orders of the FISA Court which effectively required major telecommunication companies to make disclosure of daily telephone call records on a vast and undifferentiated scale, while the company in question was itself prevented from disclosing the existence or the nature of the order. Yet the essentially secret and *ex parte* nature of the FISA Court's activities makes an independent assessment of its orders and jurisprudence all but impossible. This is another factor which must - to some degree, at least - cast a shadow over the extent to which non-US data subjects enjoy effective data protection rights in that jurisdiction so far as generalised and mass State surveillance of interception of communications is concerned.

V

16. The applicant, Mr. Schrems, is an Austrian post-graduate law student at the University of Vienna who is plainly deeply concerned about data protection security and data protection law. He is also since 2008, a user of the social network, Facebook. Although Facebook Inc. ("Facebook") is a major US company based in California, all Facebook users in Europe are required to enter into an agreement with Facebook Ireland Ltd. ("Facebook Ireland"). To that extent, therefore, Facebook Ireland falls to be regulated by the respondent Data Protection Commissioner under the terms of the Data Protection Acts, 1988-2003.

17. The practical effect of this is that Facebook Ireland is designated as a "data controller" within the meaning of s. 2 of the Data Protection Act 1988 for personal data relating to Facebook subscribers resident in the member states of the European Economic Area ("EEA"). It is not in dispute that while Facebook Ireland is subject to regulation under the Data Protection Acts, some or all data relating to Facebook subscribers resident within the EEA is in fact transferred to and held on servers which are physically located in the United States.

18. Mr. Schrems has already made some 22 other complaints concerning Facebook Ireland to the Commissioner, but it is agreed none of these fall to be considered in the present judicial review proceedings. This case rather concerns the 23rd complaint which

Mr. Schrems made concerning Facebook Ireland. This particular complaint was dated 25th June, 2013, and arose directly out of the Snowden revelations and, specifically, the PRISM programme.

VI

19. The office of the Data Protection Commissioner was established by s. 9 of the Data Protection Act 1988 ("the 1988 Act"). The 1988 Act itself has been subsequently amended in an extensive fashion, not only by the Data Protection (Amendment) Act 2003, but by a variety of other statutes and ministerial regulations which are designed to transpose EU legislation in this area.

20. Section 11(1) of the 1988 Act articulates a general prohibition on the transfer of personal data outside of the State, save where that foreign State "ensures an adequate level of protection for the privacy and the fundamental rights and freedoms of data subjects in relation to the processing of personal data having regard to all the circumstances surrounding that transfer." The reference here to privacy and the fundamental rights and freedoms of data subjects must be gauged in the first instance by the protections afforded in this regard by the Constitution, a topic to which I will presently revert.

21. So far as these proceedings are concerned, however, the critical sub-section is that contained in s. 11(2) of the 1988 Act, a sub-section which allows for the pre-emption of Irish law by EU law where a "Community finding" as to the adequacy of data protection in the third country has been made by the European Commission. Section 11(2)(a) accordingly provides:

> "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."

22. The term "Community finding" is defined by s. 11(2)(b) as meaning:

> "…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."

23. The Directive is defined by s. 1(1) as meaning the Data Protection Directive, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (O.J. L281/38)("the 1995 Directive"). Article 25(6) of the 1995 Directive provides that:

> "The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitment it has entered into, particularly upon conclusions of the negotiations referred to in paragraph 5, for the protection of private lives and basic freedoms and rights of individuals.
>
> Member States shall take the measures necessary to comply with the

Commission's decision."

24. The European Commission did adopt such a decision on 26th July, 2000 (2000/520/EC)(O.J. L 215, 25th August, 2000), citing Article 25(6) of the 1995 Directive as the legal basis for this decision. The date of this decision is, perhaps, of some significance, given that it was taken some months before the EU Charter of Fundamental Rights was adopted at Nice in December 2000 and it ante-dated by several years the coming into force of the Lisbon Treaty on 1 December 2009, which is the date on which the Charter itself was first given legally justiciable status.

25. As the recitals to that Commission decision make clear, however, an adequate level of protection:

> "for the transfer of data from the Community to the United States recognised by this Decision, should be attained if organisations comply with the safe harbour privacy principles for the protection of personal data transferred from a Member State to the United States...and the frequently asked questions ["FAQs"]…providing guidance for the implementation of the Principles issued by the Government of the United States on 21st July 2000. Furthermore, the organisations should publicly disclose their privacy policies and be subject to the jurisdiction of the Federal Trade Commission under section 5 of the Federal Trade Commission Act which prohibits unfair or deceptive acts or practices in or affecting commerce, or that of another statutory body that will effectively ensure compliance with the Principles implemented in accordance with the FAQs."

26. Article 1(2) of the decision then provides that:

> "In relation to each transfer of data the following conditions shall be met:
>
> > (a) the organisation receiving the data has unambiguously and publicly disclosed its commitment to comply with the Principles implemented in accordance with the FAQs;
> >
> > (b) the organisation is subject to the statutory powers of a government body in the United States listed in Annex VII to this Decision which is empowered to investigate complaints and to obtain relief against unfair or deceptive practices as well as redress for individuals, irrespective of their country of residence or nationality, in the case of non-compliance with the Principles implemented in accordance with the FAQs."

27. Article 1(3) then provides for a self-certification procedure:

> "The conditions set out in paragraph 2 are considered to be met for each organisation that self-certifies its adherence to the Principles implemented in accordance with the FAQs from the date on which the organisation notifies to the US Department of Commerce (or its designee) the public disclosure of the commitment referred to in paragraph 2(a) and the identity of the government body referred to in paragraph 2(b)."

28. In terms of potential enforcement of these principles, Article 3 of the Decision is perhaps the most critical provision of all:

> "Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to provisions other than Article 25 of Directive 95/46/EC, the competent authorities in Member States may exercise their existing powers to suspend data flows to an organisation that has self-certified its adherence to the Principles implemented in accordance with the FAQs in order to protect individuals with regard to the processing of their personal data in cases where:

(a) the government body in the United States referred to in Annex VII to this Decision or an independent recourse mechanism within the meaning of letter (a) of the Enforcement Principle set out in Annex I to this Decision has determined that the organisation is violating the Principles implemented in accordance with the FAQs; or

(b) there is a substantial likelihood that the Principles are being violated; 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; the continuing transfer would create an imminent risk of grave harm to data subjects; and 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.

The suspension shall cease as soon as compliance with the Principles implemented in accordance with the FAQs is assured and the competent authorities concerned in the Community are notified thereof."

VII

The complaints made by Mr.Schrems of 25th June, 2013

29. The complaint made by Mr. Schrems on 25th June, 2013, was, in essence, that by transferring user data to the United States, Facebook Ireland was facilitating the processing of such data by Facebook itself. While Facebook has self-certified by reference to the Safe Harbour principles, Mr. Schrems contended that the Snowden revelations regarding the Prism programme demonstrated that there was no meaningful protection in US law or practice in respect of data so transferred so far as State surveillance was concerned. Specifically, Mr. Schrems maintained that this was especially so given that the US law enforcement agencies could obtain access to such data without the need for a court order, or, at least, a court order showing probable cause that a particular data subject had engaged in illegal activities or stood possessed of information which would be of genuine interest to law enforcement bodies.

30. The response of the Commissioner to this complaint can probably be best summed up in a letter dated 26th July, 2013:

"...we would reiterate that the 'Safe Harbour' agreement stands as a formal decision of the EU Commission...under Article 25(6) of the Data Protection Directive 95/46/EC that the agreement provides adequate protection for personal data transferred from the EU to the USA. Section 11(2) of the (Irish) Data Protection Acts which we consider faithfully reflects our obligation to accept 'adequacy' decisions provides that

'Where in any proceedings under this Act a question arises:

(i) whether the adequate level of protection specified in sub-section (1) of this section is ensured by a country or territory outside the European Economic Area to which personal date are to be transferred, and

(ii) a Community finding has been made in relation to transfers of this kind, the question shall be determined in accordance with that finding.'

> The Commissioner has concluded that, as Facebook-Ireland is registered under the Safe Harbour arrangement and as this provides for US law enforcement access, there is nothing for this Office to investigate."

31. On the previous day, 25th July, 2013, the Commissioner had further explained by letter the approach which he was taking:

> "Section 10(1)(a) of the Data Protection Acts provides that the Commissioner "*may* investigate whether any of the provisions of [the] Act...have, are being or are likely to be contravened in relation to an individual either where the individual complaints to him of a contravention of any of those provisions or he is otherwise of opinion that there may be such a contravention." As the Commissioner is satisfied that there is no evidence of a contravention in this case, he has exercised his discretion not to proceed to a formal investigation under s. 10(1)(b) of the Acts. In making this assessment the Commissioner is also 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. The situation in this respect is quite different to that in relation to the 22 complaints you submitted earlier which related to terms and conditions of Facebook-Ireland which clearly apply to you as user."

32. In essence, therefore, it is clear that the Commissioner formed the view that as Facebook had self-certified under the Safe Harbour regime and as there was a Community finding that the Safe Harbour regime provided adequate data protection, there was nothing left for him to investigate. The Commissioner accordingly exercised his power not to investigate the matter further under s. 10(1)(b) of the 1988 Act on the basis that the complaint was "frivolous and vexatious".

33. It should also be pointed out that the Commissioner had, in any event, raised the question of the PRISM allegations with Facebook Ireland in advance of receiving Mr. Schrem's complaint. In the course of those discussions, Facebook Ireland confirmed that its parent, Facebook, did not provide access to US security agencies to subscriber data, save by means of targeted requests which were properly and lawfully made. The Commissioner had satisfied himself on the basis of an audit which he had carried out of Facebook Ireland that it had appropriate procedures in place for the handing of access requests received from security agencies generally.

VIII

Whether the complaint was "frivolous and vexatious"

34. Section 10(1) of the 1988 Act provides as follows:-

> "(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."

35. The jurisdiction of the Commissioner not to investigate complaints further under s. 10(1)(b) has been very helpfully examined by Birmingham J. in his judgment in *Novak v. Data Protection Commissioner* [2012] IEHC 449, [2013] 1 I.L.R.M. 207. Where the Commissioner has proceeded to the investigation stage, then an appeal will lie from that decision to the Circuit Court: see s. 26(1)(d) of the 1988 Act. It is common case, however, that no such appeal lies where the complaint is deemed to be frivolous and vexatious. In essence, therefore, the only remaining remedy which is available to Mr. Schrems is that of judicial review: can it be said that the Commissioner erred in law that in concluding that the complaint was "frivolous and vexatious"?

36. In *Novak* the issue was whether a candidate's answer paper in a professional examination constituted "personal data" within the meaning of the Data Protection Acts. The Commissioner concluded that the examination answer did not so constitute personal data and he declined to investigate the matter further. The student appealed to the Circuit Court, but in her judgment delivered on 16th November, 2010, Her Honour Judge Linnane concluded that absent a decision to proceed to investigate no such appeal lay. This decision was subsequently upheld by the decision of Birmingham J. for this Court.

37. So far as the jurisdictional issue is concerned, Birmingham J. concluded:

> "Section 10(1) seems to envisage that the following sequence of events will occur:-
>
> > (1) The Commissioner has to decide whether the matter submitted to him is frivolous or vexatious.
> >
> > (2) If the Commissioner is of the view that the matter was not frivolous or vexatious, then, unless an amicable resolution can be arranged within a reasonable time, he considers the matter and reaches a decision in relation to it and then informs the complainant of the decision that has been reached and that the decision may be appealed.
> >
> > (3) However, if the view is formed that the matter that has been submitted is frivolous or vexatious, then the Commissioner does not investigate the complaint or cause it to be investigated. In that event the procedure comes to a halt.
>
> I find myself in respectful agreement with Judge Linnane that the jurisdiction of the Circuit Court is to hear an appeal against a decision that has been arrived at after there has been an investigation. I share her view that absent investigation of the complaint and a decision in relation to the investigation, that the Circuit Court has no jurisdiction. The entitlement of an aggrieved party in the first place to submit an appeal and then of the Court to hear and determine an appeal arises only where there has been a decision of the Commissioner in relation to a complaint under section 10(1)(a). However, the Commissioner reaches a decision in relation to a complaint only if, not having decided that the matter is frivolous and vexatious, he proceeds to investigate the complaint and reaches a decision in relation thereto."

38. Birmingham J. then turned to the question of whether the Commissioner was correct

on the merits of the complaint, saying:

> "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... 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."

39. It is against this background that the present complaint falls to be evaluated. It is certainly true that in the ordinary sense of these words the present complaint - raising as it does weighty issues of transcendent importance in relation to data protection - is neither "frivolous" nor "vexatious". While in this respect the actual language of s. 10(1)(b) of the 1988 Act is somewhat unfortunate and perhaps even unhelpful, nevertheless, as Birmingham J. pointed out in *Novak*, in this particular statutory context these words also apply to a case where the claim is considered to be unsustainable in law. In fairness, the Commissioner has also been most anxious to stress - both in correspondence and in submissions advanced by his counsel, Mr. McDermott - that it is in this particular sense that the terms have been used in the present case and that they described the Commissioner's conclusion that the complaint cannot succeed.

40. We can now proceed to examine the merits of these judicial review proceedings. Before doing so, however, it is necessary to consider a preliminary point raised as an objection by the Commissioner, namely, that of *locus standi* of the complainant.

IX

The *locus standi* of the complainant

41. The Commissioner contends that as there is no evidence by which he could have concluded that the Safe Harbour Principles were in fact being violated in the case of data transfers between Facebook Ireland and Facebook, it was submitted that these complaints were essentially hypothetical and speculative in nature. Nor, it was further submitted, was any evidence ever adduced 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.

42. For my part, I do not think that this objection is well founded. The Snowden revelations demonstrate - almost beyond peradventure - that the US security services can routinely access the personal data of European citizens which has been so transferred to the United States and, in these circumstances, one may fairly question whether US law and practice in relation to data protection and State security provides for meaningful or effective judicial or legal control. It is true that Mr. Schrems cannot show any evidence that his data has been accessed in this fashion, but this is not really the gist of the objection.

43. The essence of the right to data privacy is that, so far as national law is concerned and by analogy with the protection afforded by Article 40.5 of the Constitution, that privacy should remain inviolate and not be interfered with save in the manner provided for by law, *i.e.*, by means of a probable cause warrant issued under s. 6 of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993, on the basis that the interception of such communications involving a named individual is necessary in the interests of either the suppression of serious crime or the protection of

national security.

44. This is also clearly the position under EU law as well, a point recently confirmed by the Court of Justice in Case C-293/12 *Digital Rights Ireland* in a case where the Data Retention Directive, Directive 2006/24/EC was held to be invalid by reason of the absence of sufficient safeguards in respect of the accessing of such data by national authorities:

> "By requiring the retention of the data listed in Article 5(1) of Directive 2006/24 and by allowing the competent national authorities to access those data, Directive 2006/24, ...derogates from the system of protection of the right to privacy established by Directives 95/46 and 2002/58 with regard to the processing of personal data in the electronic communications sector, directives which provided for the confidentiality of communications and of traffic data as well as the obligation to erase or make those data anonymous where they are no longer needed for the purpose of the transmission of a communication, unless they are necessary for billing purposes and only for as long as so necessary.
>
> To establish the existence of an interference with the fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way (see, to that effect, Cases C 465/00, C 138/01 and C 139/01 *ÖsterreichischerRundfun and Others* EU:C:2003:294, paragraph 75).
>
> As a result, the obligation imposed by Articles 3 and 6 of Directive 2006/24 on providers of publicly available electronic communications services or of public communications networks to retain, for a certain period, data relating to a person's private life and to his communications, such as those referred to in Article 5 of the directive, constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter.
>
> Furthermore, the access of the competent national authorities to the data constitutes a further interference with that fundamental right….Accordingly, Articles 4 and 8 of Directive 2006/24 laying down rules relating to the access of the competent national authorities to the data also constitute an interference with the rights guaranteed by Article 7 of the Charter.
>
> Likewise, 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.
>
> It must be stated that the interference caused by Directive 2006/24 with the fundamental rights laid down in Articles 7 and 8 of the Charter is… and it must be considered to be particularly serious. Furthermore, as the Advocate General has pointed out in paragraphs 52 and 72 of his Opinion, the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance."

45. The same reasoning applies here. Quite obviously, Mr. Schrems cannot say whether his own personal data has ever been accessed or whether it would ever be accessed by the US authorities. But even if this were considered to be unlikely, he is nonetheless certainly entitled to object to a state of affairs where his data are transferred to a jurisdiction which, to all intents and purposes, appears to provide only a limited protection against any interference with that private data by the US security authorities.

46. It is manifestly obvious that the present case raises issues of both national and EU law, although in the event the issue is largely governed by EU law given the central importance of the Commission decision of July 2000. It may nevertheless be convenient to consider the position both from the perspective of national law and EU law.

X

The position under national law

47. As far as Irish law is concerned, the accessing of private communications by the State authorities through interception or surveillance directly engages the constitutional right to privacy: see, *e.g., Kennedy v. Ireland* [1987] I.R. 587; *People v. Dillon* [2003] 1 I.L.R.M. 531 and *People v. Idah* [2014] IECCA 3. As Hamilton P. noted in *Kennedy*, this constitutional right is underscored by the Preamble's commitment to the protection of the "dignity and freedom of the individual" and the guarantee of a democratic society contained in Article 5 of the Constitution.

48. One might add that the accessing by State authorities of private communications generated within the home - whether this involves the accessing of telephone calls, internet use or private mail - also directly engages the inviolability of the dwelling as guaranteed by Article 40.5 of the Constitution. As it happens, by one of those accidents of legal history, these very same words are also contained in Article 13(1) of the German Basic Law ("inviolability of the dwelling") ("unverletzlichkeit der Wohnung"). It is, accordingly, of interest that the German Constitutional Court has held that the accessing by state authorities of otherwise private communications within the home also engages that more or less identically worded guarantee of inviolability of the dwelling which is contained in Article 13(1) of the Basic Law. Indeed that Court went further and found that legislation providing for the interception and surveillance of communications partly unconstitutional because it provided for a disproportionate interference without adequate safeguards with that very guarantee of inviolability of the dwelling in Article 13(1) of the Basic Law: see *Anti-Terrorism Database Law decision* (1 B v R 1215/07)(April 24, 2013) at paras. 93 *et seq*.

49. Naturally, the mere fact that these rights are thus engaged does not necessarily mean that the interception of communications by State authorities is necessarily or always unlawful. The Preamble to the Constitution envisages a "true social order" where the "dignity and freedom of the individual may be assured", so that both liberty and security are valued. Provided appropriate safeguards are in place, it would have to be acknowledged that in a modern society electronic surveillance and interception of communications is indispensable to the preservation of State security. It is accordingly plain that legislation of this general kind serves important - indeed, vital and indispensable - State goals and interests: *cf*. by analogy the decision of the German Constitutional Court in the *Anti-Terrorism Database* case (at paras. 106, 131 and 133, passim) and the comments of the Court of Justice in Case C-293/12 *Digital Rights Ireland Ltd*. [2014] E.C.R. I-000 at paras. 42-44.

50. The importance of these rights is such nonetheless that the interference with these privacy interests must be in a manner provided for by law and any such interference must also be proportionate. This is especially the case in respect of the interception and surveillance of communications within the home. While the use of the term "inviolable" in respect of the dwelling in Article 40.5 does not literally mean what it says, the reference to inviolability in this context nonetheless conveys that the home enjoys the highest level of protection which might reasonably be afforded in a democratic society: see, *e.g., Wicklow County Council v. Fortune* (No.1) [2012] IEHC 406.

51. By safeguarding the inviolability of the dwelling, Article 40.5 provides yet a further

example of a *leitmotif* which suffuses the entire constitutional order, namely, that the State exists to serve the individual and society and not the other way around.

52. In this regard, it is very difficult to see how the mass and undifferentiated accessing by State authorities of personal data generated perhaps especially within the home - such as e-mails, text messages, internet usage and telephone calls - would pass any proportionality test or could survive constitutional scrutiny on this ground alone. The potential for abuse in such cases would be enormous and might even give rise to the possibility that no facet of private or domestic life within the home would be immune from potential State scrutiny and observation.

53. Such a state of affairs - with its gloomy echoes of the mass state surveillance programmes conducted in totalitarian states such as the German Democratic Republic of Ulbricht and Honecker - would be totally at odds with the basic premises and fundamental values of the Constitution: respect for human dignity and freedom of the individual (as per the Preamble); personal autonomy (Article 40.3.1 and Article 40.3.2); the inviolability of the dwelling (Article 40.5) and protection of family life (Article 41). As Hardiman J. observed in *The People v. O'Brien* [2012] IECCA 68, Article 40.5

> "...presupposes that in a free society the dwelling is set apart as a place of repose from the cares of the world. In so doing, Article 40.5 complements and re-inforces other constitutional guarantees and values, such as assuring the dignity of the individual (as per the Preamble to the Constitution), the protection of the person (Article 40.3.2), the protection of family life (Article 41) and the education and protection of children (Article 42). Article 40.5 thereby assures the citizen that his or her privacy, person and security will be protected against all comers, save in the exceptional circumstances presupposed by the saver to this guarantee."

54. One might accordingly ask how the dwelling could in truth be a "place of repose from the cares of the world" if, for example, the occupants of the dwelling could not send an email or write a letter or even conduct a telephone conversation if they could not be assured that they would not be subjected to the prospect of general or casual State surveillance of such communications on a mass and undifferentiated basis.

55. That general protection for privacy, person and security in Article 40.5 would thus be entirely compromised by the mass and undifferentiated surveillance by State authorities of conversations and communications which take place within the home. For such interception of communications of this nature to be constitutionally valid, it would, accordingly, be necessary to demonstrate that this interception of communications and the surveillance of individuals or groups of individuals was objectively justified in the interests of the suppression of crime and national security and, further, that any such interception was attended by appropriate and verifiable safeguards.

56. If this matter were entirely governed by Irish law, then, measured by these constitutional standards, a significant issue would arise as to whether the United States "ensures an adequate level of protection for the privacy and the fundamental rights and freedoms" of data subjects, such as would permit data transfers to that country having regard to the general prohibition contained in s. 11(1) of the 1988 Act and the constitutional principles I have just set out. Certainly, given what I have already described as the (apparently) limited protection given to data subjects by contemporary US law and practice so far as State surveillance is concerned, this would indeed have been a matter which the Commissioner would have been obliged further to investigate.

57. It is, however, agreed, that the matter is only partially governed by Irish law and that, in reality, on this key issue Irish law has been pre-empted by general EU law in this area. This is because s. 11(2)(a) of the 1988 Act (as substituted by s. 12 of the Data Protection (Amendment) Act 2003) effects a *renvoi* of this wider question in favour of EU

law. Specifically, s. 11(2)(b) of the 1988 Act provides that the Commissioner must determine the question of the adequacy of protection in the third State "in accordance" with a Community finding made by the European Commission pursuant to Article 25 of the 1995 Directive. It is accordingly for this reason that we must therefore turn to a consideration of the position at EU law.

XI

The position under EU law

58. The position under EU law is equally clear and, indeed, parallels the position under Irish law, albeit perhaps that the safeguards for data protection under the EU Charter of Fundamental Rights thereby afforded are perhaps even more explicit than under our national law. These fundamental protections are contained in Article 7 and Article 8 of the EU Charter of Fundamental Rights. Article 7 provides:

> "*Respect for private and family life*
>
> Everyone has the right to respect for his or her private and family life, home and communications."

59. Article 8 provides:

> *Protection of personal data*
>
> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority."

60. Given that the validity of the administrative decision taken by the Commissioner is contingent on the proper interpretation and application of a Directive and, indeed, a Commission Decision taken pursuant to that Directive, it is plain that this is a case concerning the implementation of the EU law by a Member State within the meaning of Article 51(1) of the Charter, sufficient - at least so far as this part of the case is concerned - to trigger the application of the Charter: see, *e.g.*, Cases C-411/10 and C-493/10 N.S. [2011] E.C.R. I - 13991, paras. 64-69.

61. In *Digital Rights Ireland* the Court of Justice held that the Data Retention Directive was invalid, precisely because not only did it not contain appropriate safeguards, but it failed to provide for the retention of the data within the European Union with supervisions by an independent authority in the manner required by Article 8(3) of the Charter. As the Court observed (at paras. 65-69):

> "It follows from the above that Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.

> Moreover, as far as concerns the rules relating to the security and protection of data retained by providers of publicly available electronic communications services or of public communications networks, it must be held that 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. Furthermore, a specific obligation on Member States to establish such rules has also not been laid down.
>
> Article 7 of Directive 2006/24, read in conjunction with Article 4(1) of Directive 2002/58 and the second subparagraph of Article 17(1) of Directive 95/46, does not ensure that a particularly high level of protection and security is applied by those providers by means of technical and organisational measures, but permits those providers in particular to have regard to economic considerations when determining the level of security which they apply, as regards the costs of implementing security measures. In particular, Directive 2006/24 does not ensure the irreversible destruction of the data at the end of the data retention period.
>
> In the second place, it should be added that that directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data...
>
> Having regard to all the foregoing considerations, it must be held that, by adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter."

62. Judged by these standards, it is not immediately apparent how the present operation of the Safe Harbour Regime can in practice satisfy the requirements of Article 8(1) and Article 8(3) of the Charter, especially having regard to the principles articulated by the Court of Justice in *Digital Rights Ireland*. Under this self-certification regime, personal data is transferred to the United States where, as we have seen, it can be accessed on a mass and undifferentiated basis by the security authorities. While the FISA Court doubtless does good work, the FISA system can at best be described as a form of oversight by judicial personages in respect of applications for surveillance by the US security authorities. Yet the very fact that this oversight is not carried out on European soil and in circumstances where the data subject has no effective possibility of being heard or making submissions and, further, where any such review is not carried out by reference to EU law are all considerations which would seem to pose considerable legal difficulties. It must be stressed, however, that neither the validity of the 1995 Directive nor the Commission Decision providing for the Safe Harbour Regime are, as such, under challenge in these judicial review proceedings.

63. The Safe Harbour Regime was, of course, not only drafted before the Charter came

into force, but its terms may also reflect a somewhat more innocent age in terms of data protection. This Regime also came into force prior to the advent of social media and, of course, before the massive terrorist attacks on American soil which took place on September 11th, 2001. Outrages of this kind - sadly duplicated afterwards in Madrid, London and elsewhere - highlighted to many why, subject to the appropriate and necessary safeguards, intelligence services needed as a matter of practical necessity to have access to global telecommunications systems in order to disrupt the planning of such attacks.

XII

Conclusions

64. This brings us to the nub of the issue for the Commissioner. He is naturally bound by the terms of the 1995 Directive and by the 2000 Commission Decision. Furthermore, as the 2000 Decision amounts to a "Community finding" regarding the adequacy of data protection in the country to which the data is to be transferred, s. 11(2)(a) of the 1988 Act (as amended) requires that the question of the adequacy of data protection in the country where the data is to be so transferred "shall be determined in accordance with that finding." In this respect, s. 11(2)(a) of the 1988 Act faithfully follows the provisions of Article 25(6) of the 1995 Directive.

65. All of this means that the Commissioner cannot arrive at a finding inconsistent with that Community finding, so that if, for example, the Community finding is to the effect that a particular third party state has adequate and effective data protection laws, the Commissioner cannot conclude to the contrary. The Community finding in question was, as we have already seen, to the effect that the US does provide adequate data protection for data subjects in respect of data handled or processed by firms (such as Facebook Ireland and Facebook) which operate the Safe Harbour regime.

66. It follows, therefore, that if the Commissioner cannot look beyond the European Commission's Safe Harbour Decision of July 2000, then it is clear that the present application for judicial review must fail. This is because, at the risk of repetition, the Commission has decided that the US provides an adequate level of data protection and, as we have just seen, s. 11(2)(a) of the 1998 Act (which in turn follows the provisions of Article 25(6) of the 1995 Directive) ties the Commissioner to the Commission's finding. In those circumstances, any complaint to the Commissioner concerning the transfer of personal data by Facebook Ireland (or, indeed, Facebook) to the US on the ground that US data protection was inadequate would be doomed to fail.

67. This finding of the Commission is doubtless still true at the level of consumer protection, but, as we have just seen, much has happened in the interval since July 2000. The developments include the enhanced threat to national and international security posed by rogue States, terrorist groupings and organised crime, disclosures regarding mass and undifferentiated surveillance of personal data by the US security authorities, the advent of social media and, not least from a legal perspective, the enhanced protection for personal data now contained in Article 8 of the Charter.

68. While the applicant maintains that the Commissioner has not adhered to the requirements of EU law in holding that the complaint was unsustainable in law, the opposite is in truth the case. The Commissioner has rather demonstrated scrupulous steadfastness to the letter of the 1995 Directive and the 2000 Decision.

69. The applicant's objection is, in reality, to the terms of the Safe Harbour Regime itself rather than to the manner in which the Commissioner has actually applied the Safe Harbour Regime. There is, perhaps, much to be said for the argument that the Safe Harbour Regime has been overtaken by events. The Snowden revelations may be thought

to have exposed gaping holes in contemporary US data protection practice and the subsequent entry into force of Article 8 of the Charter suggests that a re-evaluation of how the 1995 Directive and 2000 Decision should be interpreted in practice may be necessary. It must be again stressed, however, that neither the validity of the 1995 Directive nor the validity of the Commission's Safe Harbour decision have, as such, been challenged in these proceedings.

70. Although the validity of the 2000 Decision has not been directly challenged, the essential question which arises for consideration is whether, *as a matter of European Union law*, the Commissioner is nonetheless absolutely bound by that finding of the European Commission as manifested in the 2000 Decision in relation to the adequacy of data protection in the law and practice of the United States having regard in particular *to the subsequent entry into force of Article 8 of the Charter*, the provisions of Article 25(6) of the 1995 Directive notwithstanding. For the reasons which I have already stated, it seems to me that unless this question is answered in a manner which enables the Commissioner either to look behind that Community finding or otherwise disregard it, the applicant's complaint both before the Commissioner and in these judicial review proceedings must accordingly fail.

71. Given the general novelty and practical importance of these issues which have considerable practical implications for all 28 Member States of the European Union, it is appropriate that this question should be determined by the Court of Justice. In these circumstances, I propose to refer the following questions to that Court in accordance with Article 267 TFEU:

> "Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in Commission Decision of 26 July 2000 (2000/520/EC) having regard to Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union (2000/C 364/01), the provisions of Article 25(6) of Directive 95/46/EC notwithstanding? Or, alternatively, may the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission Decision was first published?"

72. In these circumstances, the present proceedings must stand adjourned pending the outcome of the Article 267 reference.

XIII

Summary of overall conclusions

73. It remains only to summarise my principal conclusions:

74. First, while it is clear that Mr. Schrems' complaints are not "frivolous or vexatious" in the ordinary sense of these words, these words bear a different connotation in the context of s. 10(1)(b)(i) of the 1988 Act, at least so far as the present complaint is concerned. Used in this fashion and in this context, these term mean no more than that the Commissioner had concluded that this complaint was unsustainable in law.

75. Second, Mr. Schrems enjoys *locus standi* to bring this complaint and to bring these proceedings. It is irrelevant that Mr. Schrems cannot show that his own personal data was accessed in this fashion by the NSA, since what matters is the essential inviolability of the personal data itself. The essence of that right would be compromised if the data subject

had reason to believe that it could be routinely accessed by security authorities on a mass and undifferentiated basis.

76. Third, the evidence suggests that personal data of data subjects is routinely accessed on a mass and undifferentiated basis by the US security authorities.

77. Fourth, so far as Irish law is concerned, s. 11(1)(a) of the 1988 Act forbids the transfer of personal data to a third country unless it is clear that that jurisdiction sufficiently respects and protects the privacy and fundamental freedoms of the data subjects. In this particular context of national law, the standards in question are those contained in the Constitution.

78. Fifth, the chief constitutional protections are those relating to personal privacy and the inviolability of the dwelling. The general protection for privacy, person and security which is embraced by the "inviolability" of the dwelling in Article 40.5 of the Constitution would be entirely compromised by the mass and undifferentiated surveillance by State authorities of conversations and communications which take place within the home. For such interception of communications to be constitutionally valid, it would, accordingly, be necessary to demonstrate that this interception and surveillance of individuals or groups of individuals was objectively justified in the interests of the suppression of crime and national security and, further, that any such interception was attended by appropriate and verifiable safeguards.

79. Sixth, if the matter were to be measured solely by Irish law and Irish constitutional standards, then a serious issue would arise which the Commissioner would then have been required to investigate as to whether US law and practice in relation to data privacy, interception and surveillance matched these constitutional standards.

80. Seventh, in this regard, however, Irish law has been effectively pre-empted by EU law and specifically by the provisions of the 1995 Directive and the 2000 Decision establishing the Safe Harbour regime. With the July 2000 Decision the European Commission found that US data protection law and practice was sufficient to safeguard the rights of European data subjects and it is clear from Article 25(6) of the 1995 Directive that national data protection authorities must comply with findings of this nature.81. Eight, it follows, therefore, that if the Commissioner cannot look beyond the European Commission's Safe Harbour Decision of July 2000, then it is clear that the present application for judicial review must fail. This is because the Commission *has* already decided that the US provides an adequate level of data protection and, as we have just seen, s. 11(2)(a) of the 1998 Act (which in turn follows the provisions of Article 25(6) of the 1995 Directive) ties the Commissioner to the Commission's finding. In those circumstances, any complaint to the Commissioner concerning the transfer of personal data by Facebook Ireland (or, indeed, Facebook) to the US on the ground that US data protection was inadequate would be doomed to fail.

82. Ninth, while the applicant maintains that the Commissioner has not adhered to the requirements of EU law in holding that the complaint was unsustainable in law, the opposite is, in fact, in truth the case. The Commissioner has rather demonstrated scrupulous steadfastness to the letter of the 1995 Directive and the 2000 Decision.

83. Tenth, the applicant's objection is, in reality, to the terms of the Safe Harbour Regime itself rather than to the manner in which the Commissioner has actually applied the Safe Harbour Regime, although neither the validity of the 1995 Directive nor the validity of the Commission's Safe Harbour decision have, as such, been challenged in these proceedings.

84. Eleventh, in these circumstances the critical issue which arises is whether the proper interpretation of the 1995 Directive and the 2000 Commission decision should be re-evaluated in the light of the subsequent entry into force of Article 8 of the Charter and

whether, as a consequence, the Commissioner can look beyond or otherwise disregard this Community finding. It is for these reasons accordingly that I have decided to refer this question (and other linked questions) to the Court of Justice pursuant to Article 267 TFEU.
