UTRECHT JOURNAL OF
INTERNATIONAL AND EUROPEAN LAW

Shane Darcy, 'Battling for the Rights to Privacy and Data Protection in the Irish Courts' (2015) 31(80) Utrecht Journal of International and European Law 131, DOI: http://dx.doi.org/10.5334/ujiel.cv

CASE NOTE

Battling for the Rights to Privacy and Data Protection in the Irish Courts

Schrems v. Data Protection Commissioner [2014] IEHC 213 [2014]

Shane Darcy[1]

[1] Lecturer, Irish Centre for Human Rights, National University of Ireland Galway

Far-reaching mass surveillance by the US National Security Agency and other national security services has brought issues of privacy and data protection to the fore in recent years. Information and technology companies have been embroiled in this scandal for having shared, unwittingly or otherwise, users' personal data with the security services. Facebook, the world's largest social media company, has long-been criticised by privacy advocates because of its treatment of users' data. Proceedings before the Irish courts concerning the role of national data protection authorities have seen an examination of these practices in light of relevant Irish and EU law.

Keywords: Privacy; data protection; technology; intelligence; surveillance; security; Facebook; Ireland; European Union; PRISM; National Security Agency; US

When Mark Zuckerberg, the founder of Facebook, declared that privacy was no longer a 'social norm', it is safe to say that he was speaking as the CEO of one of the world's largest and most profitable social media companies, rather than as an individual who most likely seeks to limit how much of his own personal information is in the public domain. According to Zuckerberg, '[p]eople have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. […] That social norm is just something that has evolved over time'.[1] The medium has evolved significantly over the past two decades, but it is debateable as to whether our understandings of privacy have changed that much. There is of course a commercial interest for a social media company having greater access to an individual's personal information. This hunger for more information, and thus less privacy, has seen Facebook criticised for the treatment of its users' information. Such criticism became even more pronounced when it emerged that the company was implicated in the mass surveillance of the US National Security Agency; as Glenn Greenwald and Ewan MacAskill reported in the *Guardian* newspaper, the NSA has 'direct access' to Facebook's systems.[2] In the age of the internet, commercial and security interests in the mass gathering of data have seemingly aligned.

Privacy activists, most notably Max Schrems, founder of the 'Europe v. Facebook' campaign, have campaigned and taken legal proceedings regarding Facebook's insufficient protection of users' data. Perhaps surprisingly for some, Ireland has been something of a focal point for such litigation; Facebook, alongside a large number of other major multinational corporations have their European headquarters in Ireland, in large part because corporation tax rates in Ireland are lower than in the corporations' home countries. In addition, however, there is an impression in Europe that 'Ireland is buying residence of large companies with the promise of deliberately weak regulation of European personal data for which it is responsible'.[3] *Schrems* v. *Data Protection Commissioner* involved an examination of such regulation, and Justice Hogan of

[1] Bobbie Johnson, 'Privacy no longer a social norm, says Facebook founder', *The Guardian* (London, 11 January 2010)

[2] Glenn Greenwald and Ewan MacAskill, 'NSA Prism program taps in to user data of Apple, Google and others', *The Guardian* (London, 7 June 2013)

[3] 'Merkel call for data protection rules puts Ireland in spotlight: Ireland and UK seen as lowest common denominator on EU data privacy', *Irish Times* (Dublin, 16 July 2013)

the Irish High Court explained that the Edward Snowden revelations concerning NSA surveillance formed the backdrop to the case.[4] This case was directed against a statutory authority, the Irish Data Protection Commissioner, rather than Facebook itself, but Schrems has also launched a class-action suit in Austria against Facebook Ireland. The findings in such cases on the issues of privacy and data protection are of national, regional and indeed global significance.

Schrems made an application to the Irish High Court for judicial review of the Irish Data Commissioner's actions in relation to the transfer by Facebook Ireland of personal data to its parent company in the US. He was effectively seeking that the Commissioner exercise his statutory powers to prevent any transfer, given the lack of effective data protection in the US as shown by the NSA surveillance scandal.[5] The judge had to consider the respondent's claim that the European Commission's 'Safe Harbour' regime effectively required such transfers to go ahead, as it stipulated that the US' data protection regime is 'adequate and effective where the companies which transfer or process the date to the United States self-certify that they comply with the principles set down in the Commission decision'.[6] Before turning to the central issues, Judge Hogan, sitting as a single judge, noted the challenges arising for protecting data across borders:

> 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.[7]

In commenting on the preeminent role of the US in this context, the judge showed some deference to its practices, asserting that the mass surveillance 'undoubtedly saved many lives' and ensured a high level of security, while the Snowden revelations have compromised such programmes and possibly even risked lives.[8] However, he also acknowledged that the actions of the US and other authorities have involved 'an almost studied indifference to the privacy interests of ordinary citizens', whose rights have been 'seriously compromised by mass and largely unsupervised surveillance programmes'.[9] Judge Hogan accepted the veracity of the Snowden revelations, and the claim that personal data transferred to Facebook in the US was accessible to the NSA. As to judicial oversight by the US Foreign Intelligence Surveillance Court (hereafter: FISC), because its hearings are *ex parte* and held in secret, "an independent assessment of its orders and jurisprudence [is] all but impossible".[10] This casts a shadow, the judge correctly concludes, over the US system of data protection.

In turning to the role of Facebook Ireland in this context, the company is considered a 'data controller' under the Data Protection Act 1988 and is accordingly regulated by Ireland's Data Protection Commissioner. The relevant legislation prohibits the transfer of personal data outside of Ireland, unless the State in question guarantees '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'.[11] The Act also provides that any questions arising in this context must be determined in accordance with any relevant decisions of the European Commission – its decision of 26 July 2000, allowing for self-certification by organisations, being the relevant finding. Judge Hogan noted the critical provision in Article 3 of the decision, allowing States to suspend data flows if, for example, there is a 'substantial likelihood' that the Safe Harbour principles are being violated.[12] In response to the complaint from Schrems, the Irish Data Protection Commissioner 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'.[13] The Commissioner also asserted that the applicant provided no evidence that his personal data had been disclosed to the authorities in the US.[14]

---

[4] *Schrems v. Data Protection Commissioner* [2014] IEHC 213 [2014], paras 1–2
[5] *Ibid*, para 2
[6] *Ibid*
[7] *Ibid*, para 4
[8] *Ibid*, paras 5–6
[9] *Ibid,* para 8
[10] *Ibid,* paras 14–15
[11] Data Protection Act 1988, s 11(1)
[12] *Schrems v. Data Protection Commissioner* [2014] IEHC 213 [2014], para 28
[13] *Ibid,* para 30
[14] *Ibid,* para 31

The complaint by Schrems was seen as 'frivolous and vexatious' by the Data Protection Commissioner and it was on this basis that judicial review was sought.[15] Judge Hogan felt the complaint was neither frivolous nor vexatious in the ordinary sense of those words, 'raising as it does weighty issues of transcendent importance in relation to data protection', but rather that the Commissioner found that these words merely meant that the complaint was 'unsustainable in law'.[16] Judge Hogan did not find well-founded the Commissioner's claim that no evidence was available of violations of the Safe Harbour principles or of Schrem's personal data. In light of the Snowden revelations, it was fair to question whether there is 'meaning or effective judicial or legal control' in the US in relation to data protection.[17] The essence of the right to data privacy, for Judge Hogan, is 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 […] 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.[18]

Such an understanding was found in national law and the Irish Constitution, as well as in EU law. Applying the reasoning from the Court of Justice of the EU in *Digital Rights Ireland*, Judge Hogan held that even if Schrems could not show whether his data was or was likely to be accessed by the US authorities, or even it were 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.[19]

The judgement then proceeds to provide a focused analysis of both national and EU law on the subjects of privacy and data protection, albeit without reference to the relevant protections of the European Convention of Human Rights and the International Covenant on Civil and Political Rights, both of which are binding on Ireland.[20]

Looking at privacy, Judge Hogan affirmed that under Irish law, any interference with this right must be in a manner that is 'provided for by law' and in accordance with the principle of proportionality.[21] It would be very difficult, he considered, to find proportionate the 'mass and undifferentiated accessing by State authorities of personal data generated perhaps especially within the home'.[22] The judge considered the potential for abuse to be enormous, such that 'no facet of private or domestic life within the home would be immune from potential State scrutiny and observation'.[23] This was reminiscent of the practice of totalitarian regimes and comprised a state of affairs that 'would be totally at odds with basic premises and fundamental values of the Constitution'.[24] He held that if only national law were applicable to the case at hand, then the Data Protection Commissioner would have been obliged to further investigate Schrem's claim, but Irish law has been 'pre-empted by general EU law in this area'.[25] That being said, the position on data protection and privacy was 'equally clear' under EU law, with perhaps even greater protections provided for by the EU Charter of Fundamental Rights.[26] The Court of Justice had struck down the Data Retention Directive in *Digital Rights Ireland* by relying on Articles 7 and 8 of the Charter, namely, the right to private life and the right to protection of personal data.[27]

---

[15] *Ibid,* paras 32, 35
[16] *Ibid,* para 39
[17] *Ibid,* para 42
[18] *Ibid,* para 43
[19] *Ibid,* para 45
[20] European Convention for the Protection of Human Rights and Fundamental Freedoms (1950), entered into force 3 September 1953, 213 U.N.T.S. 221, E.T.S. 5; Article 17, International Covenant on Civil and Political Rights (1966), entered into force 23 March 1976, 999 U.N.T.S. 171., art 8
[21] *Schrems v. Data Protection Commissioner* [2014] IEHC 213 [2014], para 50
[22] *Ibid,* para 52
[23] *Ibid,* para 52
[24] *Ibid,* para 53
[25] *Ibid,* paras 56–57
[26] *Ibid,* para 58
[27] *Ibid,* para 61

Schrems v. *Data Protection Commissioner* centred on the interpretation and application of the relevant EU Directive by Ireland's Data Protection Commissioner. Judge Hogan expressed doubts about the extent to which the Safe Harbour "eegime" complies with Article 8 of the European Charter of Fundamental Rights concerning the protection of personal data. The part played by the FISC was seen as particularly problematic:

> [...] 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.[28]

Nevertheless, the Data Protection Commissioner was bound by the relevant European Directive and Commission Decision, which predate the Charter of Fundamental Rights, meaning that 'the Commissioner cannot arrive at a finding inconsistent with that Community finding'.[29] The national authority cannot contradict the European Commission on this question, the judgement seems to conclude. If the Commissioner cannot go beyond the Safe Harbour decision, then the application for judicial review must fail.[30] The matter did not rest there, however.

In an interesting conclusion of the case, Judge Hogan took the view that Schrem's real objection was not with the actions of the Data Protection Commissioner, but with the Safe Harbour regime itself, finding that there was 'much to be said for the argument that the Safe Harbour regime has been overtaken by events'.[31] Accordingly, a re-examination of the relevant Directive and Decision was perhaps necessary, even though their validity had not been challenged as such in the proceedings. The essential question, according to the High Court judge, was whether under EU law, the Commissioner was bound by the Commission's Finding given the subsequent entry into force of Article 8 of the Charter of Fundamental Rights. This was a matter for the Court of Justice itself to assess and Judge Hogan therefore decided to refer the following question to that Court under Article 267 of the Treaty of the Functioning of the European Union:

> 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?[32]

The proceedings in the case were thus adjourned, pending the outcome of the High Court's referral to the Court of Justice.

Schrems v. *Data Protection Commissioner* raises interesting questions regarding the interrelationship between national and EU law, and indeed the compliance of pre-existing EU Directives and Commission decisions with the fundamental rights set out in the European Charter and elsewhere. At its heart lies the concern regarding access by US security services, and others, to the massive troves of personal data accrued by Facebook. The situation is likely similar for other multinational information and technology companies with their European headquarters in Ireland, or indeed elsewhere in Europe. That such companies can 'self-certify' regarding compliance is clearly problematic from an enforcement perspective. The *Schrems* case adds to the calls for greater data protection in Europe and specifically for review of the Safe Harbour regime, something which had already been undertaken by the European Commission prior to the Irish

[28] *Ibid,* para 62
[29] *Ibid,* para 65
[30] *Ibid,* para 66
[31] *Ibid,* para 69
[32] *Ibid,* para 71

High Court judgement.[33] Following the *Digital Rights Ireland* case, a new EU Data Retention Directive can be expected in the near future. Technological developments over recent years have allowed for the unprecedented accumulation of personal data by corporations and for mass surveillance by national authorities, but have also greatly assisted those who wish to expose and campaign against aspects of these practices. The courts present a far slower and more cumbersome means of challenge, but are nevertheless important in securing legal and policy change.

[33] European Commission, 'Communication from the Commission to the European Parliament and the Council on the Functioning of the State Harbour from the Perspective of EU Citizens and Companies Established in the EU', Brussels, 27 November 2013, COM(2013) 847 final

How to cite this article: Shane Darcy, 'Battling for the Rights to Privacy and Data Protection in the Irish Courts' (2015) 31(80) Utrecht Journal of International and European Law 131, DOI: http://dx.doi.org/10.5334/ujiel.cv

Published: 27 February 2015

]u[*Utrecht Journal of International and European Law* is a peer-reviewed open access journal published by Ubiquity Press.

OPEN ACCESS