3. THE ROLE OF PROPORTIONALITY IN ASSESSING TRANS-ATLANTIC FLOWS OF PERSONAL DATA

David Lindsay*

1. INTRODUCTION

Security and law enforcement agencies have become reliant on the mass collection and analysis of data, especially personal data or potentially personal data, as an investigative tool, and often as a tool of first recourse.[1] The mass collection and processing of data is, moreover, notionally independent of the geographical or legal jurisdiction in which the data originates. These evolving practices give rise to considerable difficulties in determining the appropriate balance between national security and law enforcement objectives, on the one hand, and the protection of fundamental rights, on the other. Under the law of the European Union (the EU), the principle of proportionality is the single most important legal concept in establishing the balance between public interests, especially the interest in national security, and the fundamental rights to privacy and data privacy.[2] There are, nevertheless, significant complexities – both conceptual and practical – and unresolved issues, in satisfactorily applying this contested principle to rapidly changing social and technological circumstances, such as surveillance practices. These difficulties are exacerbated where surveillance

* Associate Professor Monash University, Australia. This chapter was improved significantly by very helpful comments from Professor Annalisa Ciampi, University of Verona, Professor Ian Brown, Oxford Internet Institute, and two anonymous referees. All errors and oversights remain my responsibility. So far as possible, the chapter is accurate to end of June 2016.

1 See, for example, Privacy and Civil Liberties Oversight Board (PCLOB), *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 2 July 2014; D. Lyon, *Surveillance After Snowden*, Polity Press, Cambridge 2015.

2 As Tranberg has observed: "The key to deciding the extent of a person's right to protection in connection with the processing of personal data has proved to lie largely in the ECJ's application of the basic principle of proportionality": C.B. Tranberg, 'Proportionality and Data Protection in the Case Law of the European Court of Justice' (2011) 1(4) *International Data Privacy Law* 239, 239.

practices cut across legal borders, including where data is transferred from one legal territory to another, such as occurs with trans-Atlantic flows of personal data.

In *Maximillian Schrems v. Data Protection Commissioner ('Schrems')*,[3] the Court of Justice of the European Union (CJEU) ruled that the Commission decision on the Safe Harbour Agreement,[4] which effectively authorised flows of personal data from the EU to the US, was invalid. The Court invalidated the decision on the basis that, contrary to Art. 25(1) of the 1995 Data Protection Directive ('DPD'),[5] the agreement failed to provide an adequate level of protection for personal data. Underpinning this conclusion, however, were concerns with the disproportionate mass and indiscriminate collection and access to personal data (including data originating in the EU) by US intelligence agencies, as revealed by the whistle-blower, Edward Snowden. While these US practices complied with the Safe Harbour Agreement, the Court, in effect, held that such widespread, unconstrained surveillance would breach the fundamental rights to privacy and data privacy guaranteed by EU law which, under CJEU jurisprudence, must be protected to a 'high level'.

This chapter explains the *Schrems* ruling, and the legal background to the ruling, from the particular perspective of the role of the principle of proportionality, as developed under EU law, in leading the Court to invalidate the Safe Harbour decision. In doing so, the chapter identifies legal difficulties and uncertainties in the application of proportionality analysis to cases involving interference with the rights to privacy and data privacy. While a cursory reading might suggest that the ruling is based almost entirely on the interpretation and application of the 'adequacy' test in Art. 25(1), this chapter contends that the ruling is better seen as an application of the CJEU's jurisprudence on fundamental rights and proportionality to the context of unconstrained state access to cross-border flows of personal data. Beyond this, the chapter addresses two fundamental conceptual issues arising from the *Schrems* ruling. First, the chapter explains and analyses the relationship between privacy and democracy in the context of contemporary surveillance practices, and the importance of an appropriately rigorous proportionality principle in reigning in apparently inexorable tendencies to unconstrained surveillance. Second, the chapter examines issues relating to the protection of rights against unconstrained

3 Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner* 6 October 2015.

4 See Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, 2000/520/EC, [2000] OJ L215 ('Safe Harbour decision').

5 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, [1995] OJ L281 (the DPD).

extra-territorial state surveillance, contending that the controversy surrounding trans-Atlantic data flows should be seen in the broader context of the obligations of territorially based states in relation to the rights of those outside of their territories.

In essence, the main argument made in the chapter is that while the proportionality principle is the proper legal framework for analysing the balance between security and rights, the principle, as a matter of both EU law and international human rights law, needs to be more rigorously defined and applied so as to establish a satisfactory balance between the protection of fundamental rights, on the one hand, and appropriate deference to institutions responsible for public policy, on the other. The importance of the proportionality principle, and the relevance of the argument presented in this chapter, are further illustrated by debates concerning the adequacy of the political agreement reached between the US and the EU, proposed to replace the Safe Harbour Agreement, known as the Privacy Shield. The chapter therefore concludes with an explanation and analysis of the Privacy Shield, especially from the perspective of whether or not it allows for disproportionate interferences with the rights of EU persons.

2. PROPORTIONALITY UNDER EU LAW

While as a principle for balancing government objectives and the protection of individual rights, proportionality is compelling, as a matter of implementation it presents considerable difficulties. At the most general level, the principle of proportionality, in the context of the protection of rights, is simply that any interference with rights must be justifiable in accordance with a legitimate objective and, in addition, the means for pursuing the objective must not involve a disproportionate interference with rights. As Barak puts it:

> There are two main justificatory conditions: an appropriate goal and proportionate means. … Proportionality therefore fulfills a dual function: On the one hand, it allows the limitation of human rights by law, and on the other hand, it subjects these limitations to certain conditions; namely – those stemming from proportionality.[6]

The implementation of the principle of proportionality in positive legal regimes is, however, both complex and contestable; such that, in the European context, it is more accurate to speak of principles of proportionality, and quite misleading to assume that, except at the most general level, there exists a single uniform notion of proportionality.

---

6 A. Barak, 'Proportionality and Principled Balancing' (2010) 4(1) *Law & Ethics of Human Rights* 2, 6.

The origins of the principle of proportionality in Europe can be traced to eighteenth and nineteenth century Prussian law, where it emerged as a principle for limiting the power of the administrative state.[7] Following the Second World War, it was accepted as a fundamental principle of German law, known as *Verhältnismassigkeit*, which still underpins the German rights-based constitution, or Basic Law.[8] Reflecting the mutual interdependence between the protection of individual rights and public interest limitations on rights, both the protection of fundamental rights[9] and the principle of proportionality[10] were later recognised as general principles of EU law in the jurisprudence of the CJEU. Article 52 of the EU Charter[11] now specifically provides that:

> Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

While the CJEU jurisprudence on fundamental rights (and, accordingly, on proportionality) draws inspiration from the constitutional traditions common to the Member States and from the European Convention on Human Rights (ECHR), the principle of proportionality under EU law differs from both the principle under the national laws of the Member States and the principle applied by the Strasbourg Court under the ECHR.[12] As formulated by the United Kingdom Supreme Court (UKSC) in *Bank Mellat v. Her Majesty's Treasury (No. 2)*,[13] the Strasbourg Court applied the following four-stage analysis in determining whether an administrative measure is proportionate:

1. whether its objective is sufficiently important to justify the limitation of a fundamental right;

---

7 M. Cohen-Eliya and I. Porat, 'American Balancing and German Proportionality: The Historical Origins' (2010) 8(2) *I•CON (International Journal of Constitutional Law)* 263; N. Emiliou, *The Principle of Proportionality in European Law: A Comparative Study*, Kluwer, The Hague 1996.

8 T. Tridimas, *The General Principles of EU Law*, 2nd ed., Oxford University Press, Oxford 2006, p. 136; The Rt. Hon. Lady Justice Arden, 'Proportionality: The Way Ahead?' [2013] *Public Law* 498, 499.

9 *International Handelsgesellschaft v. Einfurh-und Vorratsstelle Getreide*, Case C-11/70 [1970] ECR 125.

10 Case C-331/88, *R. v. Ministry of Agriculture, Fisheries and Food Ex p. Federation Europeene de la Sante Animale (FEDESA)* [1990] ECR I-4023.

11 Charter of Fundamental Rights of the European Union [2000] OJ C364/1.

12 The Rt. Hon. Lady Justice Arden, above n. 8; W. Sauter, 'Proportionality in EU Law: A Balancing Act?' TILEC Discussion Paper, DP 2013-003, 25.01.2013, http://ssrn.com/abstract=2208467.

13 *Bank Mellat v. Her Majesty's Treasury (No. 2)* [2013] UKSC 39, at [20].

2. whether it is rationally connected to the objective;
3. whether a less intrusive measure could have been used; and
4. whether, having regard to these matters and to the severity of the consequences, a fair balance has been struck between the rights of the individual and the interests of the community.

The clearest statement of the proportionality principle under EU law, on the other hand, was set out by the Luxembourg Court in the landmark *FEDESA* case, in the following terms:

> the lawfulness of the prohibition of an economic activity is subject to the condition that the prohibitory measures are appropriate and necessary in order to achieve the objectives legitimately pursued by the legislation in question; when there is a choice between several appropriate measures recourse must be had to the least onerous, and the disadvantages caused must not be disproportionate to the aims pursued.[14]

The precise elements of the proportionality test under EU law are not expressed consistently, and have been formulated in different terms by commentators and courts alike. On any formulation, however, it involves three components which, drawing on Tridimas, are as follows:[15]

1. Suitability – whether the measure is suitable to achieve a legitimate aim.
2. Necessity – whether the measure is necessary to achieve that aim, namely, whether there are other less restrictive means capable of producing the same result.
3. Proportionality *stricto sensu* – even if there are no less restrictive means, it must be established that the measure does not have an excessive effect on the applicant's interests.[16]

As the UKSC has explained in *R. (on the application of Lumsdon and others) v. Legal Services Board ('Lumsdon')*,[17] the third question (proportionality *stricto sensu)*, while sometimes addressed separately, is often omitted and incorporated into the necessity test.[18]

---

14 Case C-331/88, *R. v. Ministry of Agriculture, Fisheries and Food Ex p. Federation Europeene de la Sante Animale (FEDESA)* [1990] ECR I-4023, at [13].

15 T. Tridimas, above n. 8, p. 139. For a slightly different, four-stage, formulation see: W. Sauter, 'Proportionality in EU Competition Law' (2014) 35(7) *ECLR (European Competition Law Review)* 327.

16 As Tranberg points out, the three-part test at the EU level is analogous to the three components of the principle of proportionality under German law: C.B. Tranberg, above n. 2, 240, citing *Kreutzberg-Urteil*, PrOVG [1882] E 9, at 353.

17 *R. (on the application of Lumsdon and others) v. Legal Services Board* [2015] UKSC 41, at [33].

18 See also T. Tridimas, above n. 8, p. 139.

In its important judgment in *Lumsdon*, the UKSC provided a helpful summary of the Luxembourg jurisprudence,[19] including an explanation of the different levels of scrutiny applied by the CJEU in assessing measures adopted by EU institutions, on the one hand, and national measures implementing EU law, on the other.[20] In short, in assessing EU-level measures, the Court applies a 'manifestly inappropriate' test (as opposed to a 'least restrictive means' test), whereas in evaluating national measures that may derogate from fundamental rights and freedoms the Court applies the stricter 'less restrictive alternative' test. The main explanation for the different standards is that, where national implementation of an EU measure is concerned, the CJEU is 'concerned first and foremost with the question whether a member state can justify an interference with a freedom guaranteed in the interests of promoting the integration of the internal market, and the related social values, which lie at the heart of the EU project'.[21]

Within these broad parameters, it is important to appreciate that, under EU law, there is considerable flexibility in the application of the principle of proportionality to particular disputes.[22] As the UKSC observed in *Lumsdon:*

> any attempt to identify general principles risks conveying the impression that the court's approach is less nuanced and fact-sensitive than is actually the case. As in the case of other principles of public law, the way in which the principle of proportionality is applied in EU law depends to a significant extent upon the context.[23]

Given this background, we can now examine how the principle of proportionality has been applied in EU data privacy law.

3. PROPORTIONALITY AND EU DATA PRIVACY LAW

The significance of the legal context to the application of the principle of proportionality is nowhere better illustrated than in how the CJEU has applied the principle to cases involving the extent to which measures, whether at the EU or national levels, may interfere with the fundamental right to data privacy. The relevant legal context involves, first of all, the terms of the DPD, which under Recital (10) is aimed at ensuring a 'high level' of protection of data privacy and,

19 The CJEU is, however, the only authoritative source on the meaning of proportionality under EU law.

20 [2015] UKSC 41, at [40]–[82]. See also W. Sauter, above n. 12.

21 [2015] UKSC 41, at [37].

22 Thus, proportionality has been referred to as a 'flexi-principle': *R. (ProLife Alliance) v. British Broadcasting Corporation* [2004] 1 AC 185, at [138] per Walker LJ.

23 [2015] UKSC 41, [23].

under Art. 1, has the express objective of protecting the rights and freedoms of natural persons and, in particular, their right to privacy. This high level of protection is reinforced by the EU Charter, which must be taken into account in the interpretation of the DPD and which, in Art. 8, recognises a distinct right to data privacy, such that it is an independent right and not subsidiary to the more general right to privacy (recognised in Art. 7).

In a series of rulings, the CJEU has adopted a strict approach to the application of the necessity component of the proportionality principle in the context of determining permissible limits on the right to data privacy. The best starting point for understanding the Court's approach is the ruling in *Satamedia*.[24] That case concerned the publication of extracts of public data, including names and income brackets, by a Finnish regional newspaper. The key issue addressed by the Court concerned the balance to be struck between the rights to privacy and personal data, on the one hand, and the right to freedom of expression, on the other. Article 9 of the DPD establishes a balance by allowing exemptions or derogations for the processing of personal data 'carried out solely for journalistic purposes … only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression'. In interpreting the legislative balance in the light of the importance of the right to privacy, the CJEU stated that:

> in order to achieve a balance between the two fundamental rights, the protection of the fundamental right to privacy requires that the derogations and limitations in relation to the protection of data provided for in … [the DPD] … must apply only in so far as is strictly necessary.[25]

While the Court in *Satamedia* adopted an expansive interpretation of 'journalistic purposes', for the first time it interpreted the test for confining legitimate exceptions and derogations as requiring 'strict necessity', a concept that was expanded upon in subsequent cases.[26]

The *Satamedia* approach was further elaborated by the Court in a case involving the Common Agricultural Policy, *Schecke*.[27] In that case, the German state of Hesse had published the names of recipients of funding, their postal codes and the amounts received on a publicly accessible, searchable website. Finding that the requirement for publication of personal data under relevant EU regulations was an interference with the rights to privacy and data privacy guaranteed by the Charter, the Court turned to a consideration of whether the limitation was proportionate. Applying the 'strict necessity' test from *Satamedia*,

---

24 Case C-73/07, *Satakunnan Markkinapörssi and Satamedia* [2008] ECR I-9831.
25 Ibid., at [56].
26 C.B. Tranberg, above n. 2, 245.
27 Joined Cases C-92 and C-93/09 *Volker and Marcus Schecke Eifert* (ECJ, 9 November 2010).

the CJEU held that the regulations imposed a disproportionate interference with privacy rights as 'it is possible to envisage measures which affect less adversely the fundamental right of natural persons and which still contribute effectively to the objectives of the European Union rules in question'.[28] Accordingly, the Court ruled that, in introducing the regulations, the EU institutions had not established a proportionate balance between the transparency-related objectives of public disclosure, on the one hand, and the protection of the Art. 7 and 8 rights, on the other.

In *Digital Rights Ireland*,[29] the CJEU ruled that the 2006 Data Retention Directive,[30] which imposed mandatary metadata retention requirements for a period of up to two years on private telecommunications service providers, was invalid as a disproportionate interference with fundamental Charter rights. Turning first to the question of whether the directive interfered with the relevant rights, the Court held that both the retention requirements and the access arrangements in the directive amounted to interferences, to both the Art. 7 and 8 rights, that were 'wide-ranging' and 'particularly serious'.[31] In addition, the Court found that the mass retention and use of metadata without the data subjects being informed was likely to create a generalised feeling of constant surveillance.[32]

Although the Court held that the data retention law did not affect the 'essence' of the Charter right to privacy, as it did not concern retention of or access to communications content, and that the prevention of terrorism and crime were legitimate objectives of general interest, the case turned on an assessment of whether the interferences were proportionate. Where EU legislation is subject to judicial review on the basis of interference with fundamental rights, the Court's case law embodies a degree of flexibility in the application of the principle, depending on the area concerned, the nature of the right, the nature and seriousness of the interference and the object pursued by the interference.[33] In the circumstances of this case, the Court held that:

> in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the

28 Ibid., at [86].

29 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources* [2013] ECR I-847.

30 Directive 2006/24 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive [2006] OJ L105/54.

31 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources* [2013] ECR I-847, at [37].

32 Ibid.

33 Ibid., at [47].

> interference with the right caused by Directive 2006/24, the EU legislature's discretion is reduced, with the result that review of that discretion should be strict.[34]

Moreover, in relation to the crucial component of necessity, the Court applied the established case law on the rights to privacy and data privacy which, as explained above, permits derogations and limitations to the extent only that they are strictly necessary.[35]

As the data retention obligations under the directive applied indiscriminately to all electronic communications, and to all persons using electronic communications, even where there was no evidence of a link, however indirect, with serious crime or a threat to national security, the directive constituted an interference that was not strictly necessary.[36] Additionally, the absence of substantive and procedural safeguards in relation to access to the retained metadata rendered the interference more than strictly necessary. Taking into account the over-broad scope of the directive, and the lack of adequate safeguards, the CJEU ultimately concluded that the Data Retention Directive entailed 'a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such interference being limited to what is strictly necessary'.[37]

As these cases illustrate, the jurisprudence of the CJEU, in the context of cases alleging infringements of the fundamental rights to privacy and data privacy, has displayed an increasingly rigorous or 'rights protective' approach in the application of the proportionality principle and, in particular, its necessity component (which, as explained above, in practice often incorporates, or substitutes for, an assessment of proportionality *stricto sensu*). Concomitantly, this increased level of scrutiny has entailed progressively less deference to EU-level laws.[38]

Nevertheless, the flexibility in the application of the level of scrutiny applied by the Court gives rise to some uncertainty in the application of the principle.[39] First, there are questions about whether or not the strict scrutiny applied to infringements of rights applies to all Charter rights, or applies to some rights and not to others. To date, the strict level of scrutiny evident in cases such as those dealt with above appears to be confined to rights to non-discrimination, due process, property, and privacy and data privacy.[40] Although the CJEU

---

34 Ibid., at [48].
35 Ibid., at [52].
36 Ibid., at [59].
37 Ibid., at [65].
38 M-P. Granger and K. Irion, 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection' (2014) 39(6) *E.L. Rev. (European Law Review)* 835, 845.
39 Ibid., 846.
40 Ibid., 846.

eschews the creation of a hierarchy of rights, it seems clear, especially from recent jurisprudence, that some rights, including the rights to privacy and data privacy, have been accorded particular protection. Second, there are questions about the relationship between the nature of the interference with the relevant rights and the level of intensity of the proportionality analysis. While the Court's jurisprudence clearly establishes that the more serious an interference with rights the more likely the interference will be disproportionate, the precise relationship between the seriousness of an interference and the level of scrutiny remains uncertain. In *Digital Rights Ireland*, however, the Court clearly took the seriousness of the interference into account in applying a strict level of review. In addition, there is little guidance on the circumstances that may lead the Court to conclude that an interference is 'wide-ranging' or 'particularly serious', such as to justify strict review. Third, while the Court in *Digital Rights Ireland* emphasised the flexibility in the application of the principle of proportionality, taking into account a variety of circumstances, there is a lack of precision as to what strict review of an EU measure actually entails. As explained above, the CJEU has applied a 'manifestly inappropriate' test when assessing the proportionality of EU-level measures, giving a degree of deference to EU policy-making institutions. While it is clear that where strict review is applied the deference given to EU institutions is reduced, precisely how this might affect the 'manifestly inappropriate' analysis is not clear. A number of considerations are relevant here. As the UKSC pointed out in *Lumsdon*, the CJEU 'has not explained how it determines whether the inappropriateness of a measure is or is not manifest'.[41] Furthermore, at least in some cases, the Court has applied a 'least restrictive means' test to an EU-level measure in preference to the 'manifestly inappropriate' test, meaning that a measure will be regarded as disproportionate unless it is the least restrictive means of achieving a legitimate public interest objective.[42] It is therefore unclear whether the strict standard of review referred to in the cases culminating in *Digital Rights Ireland* is simply more likely to find a measure to be 'manifestly inappropriate', whether it entails applying a 'least restrictive means' test, or whether the standard is somewhere between the 'manifestly inappropriate' and 'least restrictive means' tests. To be clear, I am not suggesting that the Court adopt an overly-rigid approach in assessing the proportionality of an interference with fundamental rights; merely that the legal tests for scrutinising EU-level laws should be more clearly and precisely explained. The need for greater analytical precision is clearly illustrated by the substantial legal uncertainty, following the CJEU decision in *Digital Rights*

41 [2015] UKSC 41, at [42].

42 See W. Sauter, above n. 12, p. 13, citing Case C-210/03 *Swedish Match UK Ltd* [2004] ECR I-11893.

Ireland, concerning whether bulk data collection by intelligence agencies can ever be proportionate.

Bearing these observations on the application of the proportionality principle in the context of the right to data privacy in mind, we can turn to an analysis of the *Schrems* decision. Before doing so, however, it is necessary to explain some recent practices of US government security agencies in collecting and accessing personal data originating from outside the US, as revealed by Edward Snowden in 2013.

4. THE SNOWDEN REVELATIONS AND THE PRISM PROGRAMME

Starting in June 2013, the Snowden revelations altered the public understanding of the extent to which US security agencies have accessed and processed data originating from outside the US, including data sourced from the EU.[43] On 6 June 2013, one day after the publication of the first reports that the US National Security Agency (NSA) was collecting telecommunications log records from Verizon, *The Guardian* and *The Washington Post* published details of a programme, popularly known as PRISM, under which the NSA collected a range of data from large Internet companies, including Google, Microsoft and Facebook.[44] The reports, based on 41 PowerPoint slides leaked by Edward Snowden, revealed the mass collection of Internet data, including both content and metadata, under the authority of the US Foreign Intelligence Surveillance Court (the FISA Court).[45]

To date, the most comprehensive explanation of the operation of the PRISM programme is contained in a July 2014 report by the US Privacy and Civil Liberties Oversight Board (PCLOB) on surveillance programmes authorised pursuant to section 702 of the US Foreign Intelligence Surveillance Act 1978.[46]

---

43 Although, as Hogan J. in the Irish High Court observed, 'only the naïve or the credulous could really have been surprised' by the Snowden revelations, the factual details revealed by Edward Snowden confirmed suspicions and exposed disingenuous denials: *Schrems v. Data Protection Commissioner* [2014] IEHC at [4].

44 B. Gellman and L. Poitras, 'US Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program', *The Washington Post*, 6 June 2013, <https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html>; G. Greenwald and E. MacAskill, 'NSA Taps in to Internet Giants' Systems to Mine User Data, Secret Files Reveal', *The Guardian*, 6 June 2013, <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>.

45 For the slides see: PRISM/US-984XN Overview, April 2013, <https://www.aclu.org/files/natsec/nsa/20130816/PRISM%20Overview%20Powerpoiny%20Slides.pdf>.

46 PCLOB, above n. 1.

Section 702 establishes a regime under which the US Attorney General and the Director of National Intelligence may jointly authorise surveillance of non-US persons, who are reasonably believed to be located outside of the US, in order to acquire foreign intelligence information.[47] The government authorisations must be approved by the FISA Court, which operates in secret. Once approval has been given, written directives are sent to the Internet companies requiring them to assist in the collection of data.

The data collected is based on certain 'selectors', such as telephone numbers or e-mail addresses, associated with targeted persons. Once the government sends a selector to an Internet company, the company is compelled to pass on all communications sent to or from that selector. The NSA receives all of the data generated by the PRISM programme, while the CIA and FBI receive portions of the data.[48] Each of the relevant intelligence agencies has certain minimisation procedures, approved by the FISA Court, that restrict the use, retention and disclosure of the collected data.

The collection of data under the PRISM programme has been extensive. As the PCLOB report explained: 'Compared with the "traditional" FISA process …, Section 702 imposes significantly fewer limits on the government when it targets foreigners located abroad, permitting greater flexibility and a dramatic increase in the number of people who can realistically be targeted.'[49] Furthermore, according to the report, about 91 per cent of Internet communications obtained by the NSA each year are acquired from the PRISM programme,[50] with an estimated 89,138 persons being targeted in 2013.[51] While the programme is targeted at non-US persons, there is considerable incidental collection of data relating to US citizens. At the time of writing, US Senate Judiciary Committee hearings had commenced on the re-authorisation of section 702, which is currently scheduled to expire in December 2017.[52] In the context of this chapter, it is important to note that, although there has been considerable focus on the PRISM programme, it is but one of a range of US intelligence agency programmes which may involve the collection of personal data of Europeans. In particular, a range of data collection activities, the precise scope of which remain unclear, are authorised by Executive Order 12333 (EO-12333).

---

47 50 U.S.C. sec. 1881a, introduced by the FISA Amendment Act 2008. For a comprehensive explanation of the history of s. 702 see: L.K. Donohue, 'Section 702 and the Collection of International Telephone and Internet Content' (2015) 38 *Harv. J.L. & Pub. Pol'y (Harvard Journal of Law & Public Policy)* 117.

48 The collection is undertaken by the Data Intercept Technology Unit (DITU) of the FBI, acting on behalf of the NSA: PCLOB, above n. 1, p. 33.

49 PCLOB, above n. 1, pp. 9–10.

50 Ibid., pp. 33–34.

51 Ibid., p. 33.

52 'Senate Judiciary Committee holds first public review of Section 702 surveillance programs', http://www.openthegovernment.org/node/5209, 12 May 2016.

5. THE *SCHREMS* DECISION

5.1. BACKGROUND

The Snowden revelations, and especially those concerning the PRISM programme, form the background to a complaint made by the Austrian privacy activist, Maximillian Schrems, to the Irish Data Protection Commissioner (the IDPC) in June 2013. The complaint concerned the mass transfer of personal data from Facebook Ireland to its US parent, Facebook Inc. Within Europe, Facebook users are required to enter into agreements with Facebook Ireland, which stores the data on servers in Ireland and transmits the data to servers in the US. As Facebook Inc. is a company subject to authorisations under the section 702 programme, personal data transmitted by Facebook to the US may be collected and stored by the NSA. As a Facebook user, Schrems complained that Facebook Ireland was facilitating over-broad access to his personal data by US intelligence agencies and, accordingly, that the IDPC should direct Facebook Ireland to cease transferring personal data to the US.

The IDPC rejected the Schrems complaint, principally on the basis that as the transfers were authorised by the Safe Harbour Agreement between the EU and the US,[53] the Commissioner was prevented from investigating the complaint. The Safe Harbour Agreement was adopted by a decision of the Commission in July 2000, pursuant to Art. 25(6) of the DPD. While Art. 25(1) of the DPD sets out the principle that EU Member States must provide that transfer of personal data to a third country may take place only if that country ensures an adequate level of protection, Art. 25(6) establishes a mechanism for the Commission to determine that a third country ensures an adequate level of protection.

The Safe Harbour Agreement, which was negotiated between the EU and the US to ensure the viability of the trans-Atlantic transfer of personal data, consisted of a set of privacy principles, implemented in accordance with guidance provided by frequently asked questions (FAQs), both issued by the US Department of Commerce on 21 July 2000. The privacy principles included broad obligations relating to: providing notice of collection and processing of personal data; disclosure of personal data to third parties; data security and data integrity; and access to, and correction of, personal data. The scheme, intended for use by US private sector organisations receiving personal data from Europe, operated entirely by means of self-certification. As explained in the FAQs, the main mechanism for enforcing the self-regulatory scheme was by the US Federal

[53] Safe Harbour decision, above n. 4. The Safe Harbour principles appear as Annex I to the Commission decision.

Trade Commission (FTC) taking action on the basis of deceptive representations of compliance with the privacy principles.

The fourth paragraph to Annex I of the Commission decision adopting the Safe Harbour Agreement established significant derogations limiting the application of the principles. In particular, the decision allowed for derogations 'to the extent necessary to meet national security, public interest, or law enforcement requirements' and 'by statute, government regulation, or case-law that create conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance … is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation'. Moreover, Part B of Annex IV of the Commission decision provided that, in the event of conflicting obligations imposed by US law, organisations were required to comply with the US law.

Following the rejection of his complaint, Schrems applied to the Irish High Court for judicial review of the IDPC decision. The main issue before the Court was whether the Commission decision finding that the Safe Harbour Agreement provided an adequate level of protection conclusively prevented complaints about data transfers from Facebook Ireland to its US parent falling within the scope of the agreement. Hogan J., making limited distinctions between the various NSA programmes, simply concluded that, once in the US, the Facebook data was subject to 'mass and indiscriminate surveillance' by the NSA.[54] If the question were to be determined in accordance with Irish national law, the national court held that this level of mass and undifferentiated surveillance would create a serious issue as to whether it was a disproportionate interference with the fundamental rights to dignity, autonomy and privacy protected by the Irish constitution.[55]

However, as the case concerned a Commission decision made pursuant to an EU level directive and, accordingly, the implementation of EU law by a Member State, review of the IDPC decision fell to be determined by EU law, and especially by reference to the rights guaranteed by the EU Charter. Given the express protection of data privacy by Art. 8 of the Charter, mass and undifferentiated surveillance with weak judicial oversight, and with no appeal rights for EU data subjects, would likely breach the Charter. That said, the Irish data protection law, on its face, prevented the IDPC from second-guessing a Commission decision on adequacy. The key questions in the case were therefore whether the IDPC was bound by the Commission's Safe Harbour decision, which necessarily raised the issue of whether the Safe Harbour Agreement complied with EU law. In this respect, the High Court of Ireland observed that, as the Charter entered into

54 *Maximillian Schrems v. Data Protection Commissioner* [2014] IEHC 310 (18 June 2014), at [13].

55 Ibid., at [52].

effect after the Safe Harbour Agreement, it was essential to determine whether the agreement should be re-evaluated in the light of the Charter. The national court therefore referred the issue of whether the IDPC was bound by the Safe Harbour Agreement or whether, taking into account developments since the agreement, it could conduct an independent investigation, to the CJEU for a ruling.

5.2. THE CJEU RULING

On 6 October 2015, the CJEU handed down its ruling finding that, first, the Commission's Safe Harbour decision did not prevent a national supervisory authority, such as the IDPC, from examining whether or not a third country ensures an adequate level of protection and, second, that the Safe Harbour decision was, as a matter of EU law, invalid.[56]

In evaluating the powers of EU data protection regulators, the Court placed considerable emphasis on the legal requirements for national supervisory authorities to act independently, as derived both from the Charter and the DPD. In relation to the Charter while, as explained above, Art. 8 relevantly establishes an express right to data privacy, significantly, Art. 8(3) specifically requires rules protecting data privacy to be subject to control by an independent authority. Furthermore, Art. 28(1) of the DPD, which must be interpreted in light of the Charter, expressly requires national supervisory authorities to 'act with complete independence'. Consequently, although the Safe Harbour Agreement, while in force, was binding on EU Member States and their organs, the Court held that this could not prevent national regulators from independently examining, pursuant to Art. 28, claims that the transfer of personal data to third countries was in breach of the rights and freedoms conferred by the Charter. In this respect, the Court emphasised that 'the European Union is a union based on the rule of law in which all acts of its institutions are subject to review of their compatibility with, in particular, the Treaties, general principles of law and fundamental rights'.[57] Consequently, although only the CJEU has the competence to declare invalid an EU-level act, such as the Safe Harbour decision, the Court held that, if a supervisory authority were to find a breach of the Charter rights, national legislation must provide for recourse to national courts which, in turn, can make a reference to the CJEU.[58] In other words, while national supervisory authorities could not rule on the validity of the Safe Harbour Agreement, this did not prevent them from independently examining claims that the processing of personal data by third countries was in breach of Charter rights.

---

56 Ibid.
57 Ibid., at [60].
58 Ibid., at [65].

Given that the transfer of personal data by Facebook to the US complied with the Safe Harbour Agreement, the fundamental underlying question raised by the case concerned the validity of the Commission decision on adequacy, interpreting the DPD adequacy requirement in the light of the Charter. As explained above, the combination of the Art. 8 right and the express text of the DPD result in a high level of legal protection of data privacy in the EU. On this basis, the CJEU held that to comply with the adequacy test, a third country must ensure a level of protection which, while not identical, was 'essentially equivalent' to that conferred by EU Member States.[59] Furthermore, the importance given to the right to data privacy under the EU legal regime led the Court to conclude that, first, in reviewing the Safe Harbour decision, account must be taken of circumstances arising subsequent to the decision and, second, that the Commission decision should be subject to strict scrutiny.

In applying the 'manifestly inappropriate' test to EU measures, the CJEU traditionally held that the assessment must be made at the time of the adoption of the measure, as future effects of rules cannot be predicted with accuracy. In *Jippes*, for example, the Court stated that:

> Where the Community legislature is obliged to assess the future effects of rules to be adopted and those effects cannot be accurately foreseen, its assessment is open to criticism only if it appears manifestly incorrect in the light of the information available to it at the time of the adoption of the rule in question.[60]

In *Gaz de France – Berliner Investissements*,[61] however, the Court appeared to open the door to consideration of factors arising after the adoption of a measure in certain limited circumstances. Given that the Snowden revelations concerning widespread collection and access to data by US government authorities occurred long after the Safe Harbour decision, the extent to which subsequent developments can be taken into account in assessing the validity of the decision was especially important. The legal issues were dealt with in some detail in the advisory opinion of Advocate General Bot.[62]

Taking advantage of the limited qualification to the rule against retrospective assessment allowed in *Gaz de France*, the Advocate General emphasised the particular characteristics of a Commission decision on adequacy which favour its assessment by reference to circumstances in existence at the time of the ruling rather than the time of the adoption of the measure. In sum, the Advocate General concluded that as a decision on adequacy is intended to have an ongoing effect,

---

59 Ibid., at [74].

60 Case C-189/01 *Jippes and Others* [2001] ECR I-5689, at [84].

61 Case C-247/08, *Gaz de France – Berliner Investissements* EU:C:2009:600.

62 *Maximillian Schrems v. Data Protection Commissioner*, Case C-362/14, Opinion of Advocate General Bot, 23 September 2015.

whether or not the legal protection provided by a third country is adequate must 'evolve according to the factual and legal context prevailing in the third country'.[63] Therefore, even though the continuation in force of a Commission decision amounts to an implied confirmation of the original assessment, where a reference has been made to the Court to determine the validity of a Commission decision, taking into account the ongoing effect of the decision the Court can appropriately examine circumstances that have arisen since the decision was adopted, which may cast doubt on the continued validity of the decision.[64] In its ruling, the CJEU essentially confirmed the approach adopted by the Advocate General, such that an adequacy decision must be reviewed in the light of legal and factual circumstances that may have arisen since the decision was adopted.[65] In effect, the Court is not merely reviewing the original adequacy decision, but the Commission's ongoing obligation to review the adequacy of third country protection, taking into account changing circumstances.

Referring by analogy to the ruling in *Digital Rights Ireland*, the Court held that, in view of the importance of the protection of personal data in the context of the fundamental right to privacy, review of the Commission's adequacy decision should be strict.[66] Applying this standard, the CJEU identified a number of inadequacies with the Safe Harbour arrangements, especially in relation to the processing of data pursuant to the NSA programmes. For example, self-certification under the arrangements is available only to US 'organisations', which means that the principles do not apply to US public authorities.[67] More importantly, the national security, public interest and law enforcement derogations under Annex I, referred to above, effectively meant that these interests could prevail over the fundamental rights of EU data subjects. As the Court put it, the derogations meant that the Safe Harbour decision:

> enables interference, founded on national security and public interest requirements or on domestic legislation of the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States.[68]

Moreover, as far as procedural safeguards were concerned, the Safe Harbour arrangements provided for enforcement only in relation to commercial disputes, with no safeguards whatsoever against state interference with fundamental rights.

---

63 Ibid., at [134].
64 Ibid., at [136].
65 Ibid., at [76].
66 Ibid., at [78].
67 Ibid., at [82].
68 Ibid., at [87].

Accordingly, the combination of the broad derogations for public security and law enforcement, with a lack of legal remedies for access by state authorities, led the Court to conclude that the Safe Harbour Agreement failed to provide adequate protection under Art. 25 of the DPD, when read in the light of the Charter. In particular, the broad derogations were not limited to what was strictly necessary for the legitimate objectives of national security and law enforcement, as they enabled generalised, undifferentiated storage of, and access to, personal data, without any limiting criteria. As the Court put it, citing *Digital Rights Ireland:*

> Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail…[69]

From this, the CJEU concluded that the generalised access enabled by the Safe Harbour Agreement compromised the essence of the fundamental right to privacy guaranteed by Art. 7 of the Charter.[70] Moreover, the lack of legal recourse for state intrusions, such as the NSA surveillance, compromised the essence of the fundamental right to effective judicial protection, guaranteed by Art. 47 of the Charter.[71] Finally, Art. 3 of the Safe Harbour decision, which effectively limited the circumstances in which national supervisory authorities may suspend data flows to self-certifying organisations, impermissibly denied the power of supervisory authorities to independently examine complaints that a third country does not ensure an adequate level of protection.[72] In short, on a number of bases, but especially on the grounds that the Safe Harbour Agreement did not provide satisfactory protection against surveillance by US government authorities, the CJEU ruled that the Commission decision on adequacy was invalid.

While, on a superficial reading, it might appear that the CJEU ruling is based entirely on an interpretation of the adequacy requirement in Art. 25(1) of the DPD, a closer reading indicates that it is a ruling on the proportionality of extra-territorial state data surveillance, in which the Court builds upon previous rulings determining whether or not an infringement of the Art. 7 and 8 rights

69 Ibid., at [93].
70 Ibid., at [94].
71 Ibid., at [95].
72 Ibid., at [102].

is proportionate to emphasise the need for any derogations or limitations on the protection of personal data to be confined to what is strictly necessary. This interpretation follows from the following reasoning: the high level of protection of data privacy means that 'adequate' protection must be interpreted as 'essentially equivalent' protection; therefore the proportionality analysis applied to an EU law, such as the Data Retention Directive, must be applied *ipso facto* in an 'essentially equivalent' manner to the laws of a third country in assessing whether or not that jurisdiction provides adequate protection.

That said, it must be acknowledged that the Court's explicit statements on the application of the proportionality principle are limited; one must to an extent read between the lines, taking into account the above implicit reasoning and the following three main points made by the Advocate General. First, analogous to the reasoning and language used in *Digital Rights Ireland*, the Advocate General held that the almost unfettered access to personal data enjoyed by US intelligence agencies meant that the interference with Charter rights was 'wide-ranging' and 'particularly serious'.[73] Second, distinguishing the reasoning in *Digital Rights Ireland*, the Advocate General held that, as the PRISM programme enabled access to content, the interference was such as to compromise the 'essence' of the fundamental right to privacy.[74] Third, the Advocate General applied the approach taken to the 'strict necessity' test in *Digital Rights Ireland* to effectively hold that the infringement was disproportionate as it allowed untargeted and indiscriminate access to all data, including content, of EU data subjects, without any relevant link to the general interest objective of national security.[75]

Apart from the disproportionality flowing from the undifferentiated mass access to personal data, the Court's decision on validity was, on my reading, influenced by the absence of any effective procedural safeguards, in the form of enforceable rights, available to EU data subjects. According to the jurisprudence of the CJEU, the proportionality analysis may be affected by the existence of procedural safeguards, such as where an otherwise problematic interference with rights may be found to be proportionate due to procedural guarantees.[76] In relation to the Safe Harbour decision, however, the limitation of enforcement proceedings before the FTC to commercial disputes meant that EU data subjects had no administrative or judicial means of redress against access by US government authorities. As the Court itself explained, the Commission's Safe Harbour decision completely failed to refer to 'the existence of effective

73 Ibid., at [171].
74 Ibid., at [177].
75 Ibid., at [198].
76 See W. Sauter, above n. 12, p. 14, citing Joined Cases C-154/04 and C-155/04, *The Queen, on the application of Alliance for Natural Health and Others v. Secretary of State for Health and National Assembly for Wales (Food supplements)* [2005] ECR I-6451.

legal protection' against interferences with fundamental rights resulting from measures originating from the US State.[77]

6. LEGAL EVALUATION OF THE *SCHREMS* DECISION

The EU is a legal entity based upon the rule of law which, applying the EU Charter, incorporates the protection of fundamental rights and freedoms as significant grounds for judicial review. Historically, review of EU-level measures by the CJEU, including in applying the principle of proportionality, has accorded a significant degree of deference to EU institutions. The main reason for this level of deference has been a reluctance for the Court to second-guess policy decisions which involve complex political, economic and social choices.[78] As explained above, however, since the introduction of the Charter, the Court has adopted an increasingly strict approach to rights-based review of EU measures, especially in cases involving infringements of particular rights, such as the Charter rights to privacy and data privacy. Particularly in the context of data privacy, the combination of the express Art. 8 Charter right, which may well go beyond the right to privacy protected under Art. 8 of the ECHR,[79] and the objectives of the DPD have led the Court to apply a high level of protection to data subjects. To date, this can be regarded as culminating, in *Digital Rights Ireland*, with the application of strict review to cases involving serious infringements to the rights to privacy and data privacy.

In most respects, the CJEU's ruling in *Schrems* amounts to little more than an application of the Court's approach to proportionality, especially as formulated in *Digital Rights Ireland*, to the context of the Commission's Safe Harbour adequacy decision. Applying this approach, the unconstrained derogations for national security and law enforcement in Annex I of the agreement clearly failed the strict necessity test. Moreover, the absence of any procedural safeguards against widespread access and use of personal data by US government agencies was a significant distinct consideration reinforcing the conclusion that the Safe Harbour decision was invalid as it allowed a disproportionate interference with rights. As distinct from *Digital Rights Ireland*, however, the Court held that the interference allowed by the Safe Harbour Agreement compromised the 'essence' of the relevant rights as it facilitated generalised access to communications content, as opposed to metadata.

---

77 *Maximillian Schrems v. Data Protection Commissioner*, Case C-362/14, 6 October 2015, at [89].

78 See, e.g., Case C-491/01 *R v. Secretary of State for Health, Ex p. British American Tobacco (Investments) Ltd and Imperial Tobacco Ltd* [2002] ECR I-11453.

79 See, e.g., the reasoning of the English High Court in *The Queen v. The Secretary of State for the Home Department* [2015] EWHC 2092.

Of potentially more long-term legal significance, however, may be the conclusion of the Court that the Commission decision on adequacy can be assessed taking into account factual and legal circumstances arising after the adoption of the decision. But, on this, the Court was careful to emphasise the distinctive characteristics of a decision on adequacy, which is intended to ensure a continuing and ongoing high level of protection in relation to transfers of personal data to third countries. As such, a failure of the Commission to appropriately review a decision in the light of important changes in circumstances, such as the Snowden revelations, may be as damaging to the protection of rights as a failure to adequately take into account known circumstances at the time of an original decision.

That said, the *Schrems* ruling neither adds much to, nor advances the law, in relation to significant unresolved legal issues concerning the application of the proportionality principle to contexts involving infringements to privacy and data privacy identified earlier in this chapter. In particular, it does not resolve especially difficult issues relating to whether or not the bulk, indiscriminate collection of personal data by intelligence agencies can ever be justifiable, which have been left unclear by the Court's ruling in *Digital Rights Ireland.* At the time of writing, it was hoped that these issues would be more explicitly addressed, and potentially resolved, by the CJEU in its forthcoming ruling in the joined cases of *Tele2 Sverige AB v. Post-och telestyrelsen* and *Secretary of State for the Home Department v. Davis and others;*[80] and the forthcoming advice on the validity of the draft PNR (Passenger Name Records) Canada agreement.[81] On the other hand, as explained in this chapter, the *Schrems* case does provide an important opportunity for examining these legal issues in a broader factual and legal context, especially involving the protection of rights across territorial borders, which are taken up in the sections of this chapter immediately following.

7. PROPORTIONALITY, PRIVACY RIGHTS AND DEMOCRACY

CJEU jurisprudence concerning the application of the principle of proportionately to interferences with the fundamental rights to privacy and data privacy has progressively increased the intensity of scrutiny applied to infringements and,

80 CJEU, Joined Cases C-203/15 and C-698/15. On 19 July 2016, Advocate-General Henrik Saugmandsgaard Øe issued an advisory opinion which, in part, concluded that a general data retention obligation may be compatible with EU law: ECLI:EU:C:2016:572 (19 July 2016).

81 CJEU, Case A-1/15. On 8 September 2016, Advocate-General Paolo Mengozzi issued an Advisory Opinion finding that certain provisions of the draft PNR agreement were incompatible with the EU Charter as not being sufficiently 'targeted': *Opinion 1/15*, ECLI:EU:C:2016:656 (8 September 2016).

concomitantly, decreased deference to EU-level policy-making. Rights-based judicial review of legislation and policy-making, based on a relatively 'thick' concept of the rule of law,[82] such as that embodied in an expansive application of the principle of proportionality incorporating strict review, is controversial. The main objections to the effective substitution of a court's decision to that of a policy-making institution, such as a legislature, relate to the relative lack of competency of the courts to take into account the complex considerations relevant to proper policy-making, and their lack of democratic accountability.[83] This chapter is not the place to canvass these arguments; let alone to provide a satisfactory rebuttal to the claims of rights sceptics. In this section of the chapter, however, it is possible to provide some limited reflections on the protection of privacy rights by the Court, and the relationship between privacy rights and democracy, in the context of the application of the principle of proportionality to trans-Atlantic data flows.

At base, liberal democracies depend upon some degree of mutual trust between citizens and State, which appears to be increasingly precarious, especially in Western democracies.[84] The asymmetric relationship between State and citizen necessarily engenders a degree of mutual suspicion. While the liberal State has a monopoly on legitimate power, intelligence-gathering and analysis are effectively delegated to specialised security agencies (and outsourced to sub-contractors), which have a relatively independent sphere of operation. The imperatives facing security agencies invariably tend to over-reach, with an almost gravitational attraction to total information surveillance. In periods of heightened and generalised security risk, elected officials face incentives to publicly support expert security agencies, inexorably tending to capture. Once over-reach is revealed, however, trust is further eroded in what, effectively, may become a vicious cycle.

The extent to which democracies – in the loosest sense of government by representatives accountable to the people – depend upon a degree of trust draws attention to the pre-conditions for democratic government. Insufficient or ineffective limits on government intrusions on individual rights erodes the capacities of people to effectively participate in, and sustain, a democratic

---

82 See J. Goldsworthy, 'Legislative Sovereignty' in T. Campbell, K.D. Ewing and A. Tomkins (eds.), *Sceptical Essays on Human Rights*, Oxford University Press, Oxford 2001, pp. 61–78.

83 The literature, of course, is extensive. For some of the most sophisticated 'rights-sceptic' arguments see: J. Waldron, *The Dignity of Legislation*, Cambridge University Press, Cambridge 1999; M. Tushnet, *Taking the Constitution Away from the Courts*, Princeton University Press, Princeton 1999.

84 This chapter was written before the 23 June 2016 referendum resulting in a majority vote in favour of the United Kingdom withdrawing from the European Union; that vote, being contrary to the position advocated by both major parties in the UK, seems to have been, in part, attributable to the trust deficit.

polity. Although few would frame the issues in such unsophisticated terms, rights and democracy are not a zero-sum game but, in senses that count, are mutually reinforcing. In the context of mass government surveillance, if people perceive that their activities, and especially their online interactions, are being perpetually monitored, this undermines the very concepts of an engaged citizenry, democratic pluralism and free political debate. As Richards has put it:

> When the government is keenly interested in what people are saying to confidants in private, the content of that private activity is necessarily affected and skewed towards the ordinary, the inoffensive, and the boring, even if the subject of surveillance is not a terrorist. If the government is watching what we say and who we talk to, so too will we make our choices accordingly. The ability of the government to monitor our communications is a powerful one, and one that cuts to the very core of our cognitive and expressive civil liberties.[85]

To claim that rights to privacy and data privacy are essential to democracy does not, of course, entail that an expansive protection of these rights must be guaranteed by the courts. While governments have a tendency to be captured by national security agendas, as Waldron has cautioned, in times of national emergency courts have been reluctant to impose limits on government actions.[86] Nevertheless, in the absence of effective internal limits, the courts are the main candidate for imposing limits on state power. The key questions then resolve to the extent of the courts' discretion in exercising rights-based review and the bases on which such discretion is exercised. But just as the principle of proportionality arose in eighteenth and nineteenth-century Prussia as a limit on the nascent growth of the administrative state in the absence of democratically imposed constraints, so the manifest failure of democratic processes to effectively curtail the excesses of state surveillance programmes, as revealed by Edward Snowden, suggests that the legal principle of proportionality has an important role to play in filling this gap in contemporary circumstances.

While the principle of proportionality may be an appropriate lens through which to analyse the balance between security and rights, it must be acknowledged that the application of the principle, and especially the necessity test and proportionality *stricto sensu*, entails the Court substituting, at least to an extent, its own assessment of the merits of a law or policy for that of the promulgating institution.[87] The problem then becomes how effectively to limit the Court's

---

85 N.M. Richards, 'Intellectual Privacy' (2008) 87 *Texas Law Review* 387, 433. See also D. Lyon, above n. 1, pp. 107–113.

86 J. Waldron, 'Security and Liberty: The Image of Balance' (2003) 11 *Journal of Political Philosophy* 191, 191.

87 T. Tridimas, above n. 8, p. 140.

discretion, as unconstrained decision-making can easily veer to the arbitrary. The answer is that the limits must come from internal constraints imposed by the Court on itself in the form of its reasoning process, or what Stone Sweet and Mathews have described as 'an argumentation framework', meaning simply a system of reasoning that gives coherence by means of stable decision-making procedures.[88] While some, principally Alexy, claim that the proportionality balancing exercise can be conducted with almost mathematical precision,[89] it remains essential for any analysis to incorporate sufficient flexibility for the courts to remain sensitive to both significant factors that may influence the analysis and the facts of instant cases. As explained in this chapter, however, the CJEU jurisprudence applying the principle of proportionality, especially in the context of infringements of the rights to privacy and data privacy, has so far produced a degree of legal uncertainty including, importantly, in relation to the precise level of scrutiny to be applied to limitations on the rights, and whether the bulk collection of data can ever be proportionate. That said, the continued and growing importance of privacy rights to a democratic constitution, in contemporary circumstances, suggests that the Court has been correct in according less deference to EU institutions when these rights are implicated. Nevertheless, a greater degree of precision and discipline in identifying and explaining the legal constraints on the proportionality analysis would help significantly to dissipate concerns about potential judicial over-reach, as well as to add much-needed certainty.

8. PROPORTIONALITY, TRANS-ATLANTIC AND TRANSBORDER DATA FLOWS

On any approach taken to the balancing of rights and security, the mass, indiscriminate data surveillance by US government agencies, with no effective procedural safeguards, as revealed by Snowden, would be disproportionate.[90] In the online environment, however, interferences with rights, such as disproportionate surveillance by state agencies, may occur at a distance.[91] The

88 A. Stone Sweet and J. Mathews, 'Proportionality Balancing and Global Constitutionalism' (2008) 47 *Columbia Journal of Transnational Law* 73, 89–90.

89 R. Alexy, *A Theory of Constitutional Rights*, trans. J. Rivers, Oxford University Press, Oxford 2002; see also M. Klatt and M. Meister, *The Constitutional Structure of Proportionality*, Oxford University Press, Oxford 2012.

90 In Europe, these practices would be in breach of the distinct proportionality principles in national laws, as well as the principles applied by the Strasbourg and Luxembourg courts.

91 As Brown and Korff put it: 'the global infrastructure of the Internet and electronic communications has made surveillance of … extraterritorial communications easier': I. Brown and D. Korff, 'Foreign Surveillance: Law and Practice in a Global Digital Environment' (2014) 3 *European Human Rights Law Review* 243, 245.

border-transgressing features of online communications raise conspicuous problems of transborder protection of rights. As territorial legal jurisdictions commonly provide less protection to foreigners than is accorded domestic citizens and residents,[92] transborder infringements of rights commonly escape judicial rights-based review. The DPD's requirement that transfers of personal data to third countries should be permissible only where that jurisdiction provides an adequate level of protection implements the EU's obligation to protect the rights of EU data subjects irrespective of territorial borders. The mechanism whereby the Commission determines the adequacy of a legal regime of a third country, however, raises the spectre of one legal jurisdiction imposing its standards on other jurisdictions in order to ensure the flow of transborder data, which has become essential to global commerce. The Commission's decision, back in July 2000, approving the Safe Harbour Agreement was clearly a pragmatic political compromise, which accorded some protection to data subject to trans-Atlantic transfers, while ensuring the continuation of the vital transborder trade. However, as explained in this chapter, the CJEU's ruling in *Schrems* confirms that any political agreement regarding adequacy must comply with the high level of protection of the rights to privacy and data privacy guaranteed by EU law.

In an era of mass transborder data flows, questions relating to the obligations of territorially based states to protect the rights of people physically located outside of their territory have become increasingly pressing. The lacuna in legal protection clearly opens the door to mass, unconstrained interference with rights across borders. The prevalence of these practices, as revealed by Snowden, exposes a significant gap in international human rights protection. This gap is too important to leave to essentially political negotiations between state parties even where, as is the case with data flows from the EU, such agreements are subject to rights-based judicial review. While some, including the UN Human Rights Committee, interpret existing international human rights law as imposing rights-based obligations on states where their actions have extra-territorial effects,[93] the legal position is far from clear. More importantly, significant state actors, and especially the US, continue to refuse to accept that their international human rights obligations extend to actions and persons outside their territorial borders.[94]

The CJEU ruling in *Schrems* invalidating the Safe Harbour decision, and the negotiations between the EU and US concerning a replacement agreement,

---

92 For example, in *Verdugo-Urquidez*, the US Supreme Court held that the Fourth Amendment does not apply to the search and seizure by US agents of property owned by a non-resident alien and located in a foreign country: *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990).

93 United Nations Human Rights Committee, *Concluding observations on the fourth periodic report of the United States of America*, CCPR/C/USA/CO/4, p. 2.

94 I. Brown and D. Korff, above n. 91, p. 248.

should not be seen in isolation from international human rights law. Just as the principle of proportionality is applied by the Court in relation to personal data originating from the EU, transborder rights obligations should ideally apply to all transfers of personal data, of whatever origin. Applying a broad proportionality principle would ensure that the transborder surveillance practices of state actors are both appropriately targeted and incorporate sufficient procedural safeguards. Nevertheless, just as this chapter has argued for greater clarity and rigour in the development and exposition of the proportionality principle under EU law, so there is a pressing need for clarification of the position under international human rights law, and ideally for the development of an appropriate transborder framework for the application of a proportionality principle. In this, the developing jurisprudence of the CJEU may serve as a test-bed; but there clearly remains work to be done at both the EU and international levels. In this respect, it is hoped that the opportunities presented by the impending CJEU decisions involving bulk data collection will give rise to significant developments, including in appropriately refining the proportionality principle.

9. THE 'PRIVACY SHIELD' AND PROPORTIONALITY

Following the Snowden revelations, the European Commission adopted two communications identifying weaknesses with the Safe Harbour Agreement in the light of the revelations and setting out a plan for restoring trust in trans-Atlantic data flows.[95] Thereafter, in 2014, negotiations between the US and the EU commenced with a view to revising the Safe Harbour Agreement to take into account the Commission's concerns, but failed to advance due mainly to difficulties experienced in negotiating a separate agreement, known as the 'Umbrella Agreement', that was designed to deal with trans-Atlantic cooperation, including data-sharing, relating to criminal and terrorism investigations.[96]

---

95 European Commission, Communication to the European Parliament and the Council on Rebuilding Trust in EU-US Data Flows (COM(2013) 846 final) 27 November 2013; European Commission, Communication to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU (COM(2013) 847 final) 27 November 2013.

96 R. Massey and H.E. Sussman, 'The US-EU safe harbor framework is invalid: now what?' (2016) 22(1) *CTLR (Computer and Telecommunications Law Review)* 1. On 2 June 2016, representatives of the US and EU announced the signing of the 'Umbrella' agreement: European Commission, 'Joint EU-U.S. press statement following the EU-U.S. Justice and Home Affairs Ministerial Meeting', Amsterdam, 2 June 2016. The agreement was approved by the European Parliament on 1 December 2016, but implementation in the US may be complicated by the approach of the incoming Trump administration: D. Bender, 'European Parliament Approves EU-U.S. Umbrella Agreement', *Inside Privacy*, 2 December 2016, https://www.insideprivacy.com/international/european-union/european-parliament-approves-eu-u-s-umbrella-agreement/.

The *Schrems* ruling, however, made it imperative for a new agreement to be reached; and the Article 29 Working Party, which consists of data protection regulators of Member States, set the end of January 2016 as the deadline for the European Commission and the US to reach agreement before enforcement actions, arising from the invalidation of the Safe Harbour Agreement, would be taken. This section of the chapter explains and analyses the proposed replacement agreement, with a focus on the role of proportionality in assessing the adequacy of the proposed agreement.[97]

Eventually, on 2 February 2016, the European Commission and the US Department of Commerce announced that they had reached a political agreement, known as the Privacy Shield, designed to replace the Safe Harbour Agreement.[98] Nevertheless, the details of the agreement were not published until 29 February 2016, when the Commission released a communication,[99] a draft adequacy determination[100] and the annexed text of the Privacy Shield. The agreement was aimed at ensuring an adequate ('essentially equivalent') level of protection by satisfactorily addressing the problems identified by the CJEU with the Safe Harbour Agreement while, as might be expected from an international agreement, embodying a series of political compromises. Significantly, enforcement of the Privacy Shield on US organisations remains based on self-certification of compliance with privacy principles, subject to overview by the FTC.

The main features of the Privacy Shield Framework are as follows:

- A revised and strengthened set of privacy principles, including a notice principle that requires a link to the Privacy Shield List (a list of self-certifying organisations maintained by the US Department of Commerce and including organisations removed from the list) and reference to the individual right of

97 Since this chapter was written, on 8 July 2016 the European Commission adopted the final version of the Privacy Shield which came into effect on the same day: European Commission, *Commission Implementing Decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, C(2016) 4176 final, 12 July 2016. On 27 October 2016, Digital Rights Ireland lodged a challenge to the Privacy Shield before the CJEU: J. Fioretti and D. Volz, 'Privacy group launches legal challenge against EU-U.S. data pact', *reuters.com*, 27 October 2016, http://www.reuters.com/article/us-eu-dataprotection-usa-idUSKCN12Q2JK.

98 European Commission, 'EU Commission and United States agree on new framework for trans-Atlantic data flows: EU-US Privacy Shield', Press Release, 02.02.2016 <http://europa.eu/rapid/press-release_IP-16-216_en.htm?locale=en>.

99 EUROPEAN COMMISSION, Communication to the European Parliament and the Council, Transatlantic Data Flows: Restoring Trust through Strong Safeguards (COM(2016) 117 final) 20.02.2016.

100 European Commission, Draft Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, 29.02.2016.

access to personal data, and an onward transfer principle that places some limits on transfers of personal data to third parties.

- Revised enforcement and liability mechanisms, conferring greater rights on EU data subjects. The new redress mechanisms include: an obligation on self-certifying organisations to designate an independent dispute settlement body to address complaints; a commitment by the Department of Commerce to receive and undertake best efforts to resolve complaints, including receiving complaints from EU member data protection authorities; a commitment by the FTC to give priority consideration to referrals of non-compliance with the privacy principles and to receive complaints directly from individuals; and an obligation on self-certifying organisations to cooperate with EU Member State data protection authorities.
- As a 'last resort' recourse mechanism, after the exhaustion of all other avenues, binding arbitration is to be available from a Privacy Shield Panel, consisting of at least 20 arbitrators selected jointly by the US Department of Commerce and the European Commission, and which can award non-monetary equitable relief.
- Increased transparency, and overview mechanisms, of access to personal data of EU data subjects by US public authorities, including intelligence agencies. As explained in the Commission's draft adequacy decision, a range of internal and political oversight and transparency mechanisms apply to US intelligence agencies. Nevertheless, as the draft decision acknowledged, available recourse mechanisms for EU data subjects against US public authorities are limited and, in some cases, such as activities authorised under EO-12333, non-existent. To address this, in a letter from the US Secretary of State set out in Annex III of the draft decision, the US government undertook to create a Privacy Shield Ombudsperson to receive and respond to complaints about US public authorities. The proposed scheme requires individual complaints to be directed to the EU Member State bodies responsible for oversight of security services, then sent to a centralised EU complaint handling body (if created), before being referred to the Ombudsperson to investigate whether US laws have been complied with.
- Limitations and derogations from privacy principles for US public authorities for national security, public interest and law enforcement purposes. Annex II, Section I.5 to the Privacy Shield draft adequacy decision specifically provides that adherence to the privacy principles is 'limited to the extent necessary to meet national security, public interest or law enforcement requirements'.[101] Accordingly, in making a determination on adequacy, the Commission was required to assess limitations under US law relating to national security, public interest or law enforcement purposes. In particular, the Commission's draft

[101] Ibid., Recital (52).

adequacy decision refers to limitations on the activities of US intelligence agencies that have been imposed since the Snowden revelations and, especially, limitations imposed by Presidential Policy Directive 28 ('PPD-28'), a binding Presidential directive which applies to 'signals intelligence' activities, issued on 17 January 2014. According to PPD-28, signals intelligence may be collected only where there is a foreign intelligence or counterintelligence purpose and collection of personal data must always be 'as tailored as feasible'. Elaborating on this, the draft adequacy decision refers to representations of the US Office of the Director of National Intelligence ('ODNI'), in a letter set out in Annex VI to the draft decision, which explain that, while bulk collection of signals intelligence is sometimes necessary, there is a general rule preferring targeted collection.[102] In addition, the US government assured the Commission that it does not engage in 'indiscriminate surveillance' and that any bulk collection of Internet data, including via access to trans-Atlantic cables, applies only to a 'small proportion of the Internet'.[103]

- An annual joint review of the Privacy Shield framework, involving the European Commission, the US Department of Commerce and the FTC, and being open to all EU data protection authorities, resulting in a public report prepared by the Commission and submitted to the European Parliament and the Council.

Since its release, the Privacy Shield agreement has been subject to considerable analysis, and criticism, including by relevant EU-level institutions. On 13 April 2016, the Article 29 Working Party published its opinion on the Privacy Shield draft adequacy decision.[104] While welcoming the improvements made by the Privacy Shield when compared with the Safe Harbour Agreement, the Working Party identified a number of important shortcomings which, in its view, need to be resolved or clarified in order for the agreement to confer the high level of protection required for an adequacy decision. Given its focus, it is beyond the scope of this chapter to engage in a detailed critical analysis of all aspects of the complex Privacy Shield agreement. Instead, this section of the chapter concentrates on the main problems identified by the Working Party and its assessment of the extent to which the agreement satisfies the requirements of necessity and proportionality.[105]

---

102 Ibid., Recital (59).

103 Ibid., Recital (69).

104 Article 29 Data Protection Working Party, Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision, 16/EN WP 238, Adopted on 13 April 2016.

105 On 24 May 2016, the European Parliament agreed to a joint resolution on the Privacy Shield which, amongst other things, called on the European Commission to implement the recommendations made by the Article 29 Working Party in its Privacy Shield opinion: European Parliament, Joint Motion for a Resolution pursuant to Rule 123(2) and (4) of

Overall, the Working Party considered that the format adopted by the Privacy Shield, with the relevant principles and guarantees being set out in both the adequacy decision and annexes to the decision, resulted in a lack of clarity and, at times, inconsistency.[106] Consequently, the Working Party called for further clarification and consistency in the draft decision, including the preparation of a glossary of terms. In relation to transfers of personal data by commercial organisations, the Working Party pointed to significant omissions in the privacy principles when compared with EU data privacy law, including the lack of a data retention limitation principle, requiring organisations to delete data if they are no longer necessary, and a lack of legal guarantees for individuals subject to automated decisions which produce legal effects or otherwise significantly affect an individual.[107] On the key issue of limitations and derogations from the privacy principles for US public authorities, the Working Party engaged in an analysis of the relevant US legal framework, including PPD-28, EO-12333 and the ODNI letter set out in Annex VI to the Commission's draft decision. While acknowledging the significant steps taken by the US to increase transparency of the practices of security agencies since the Snowden revelations, the Working Party concluded that, in important respects, the draft adequacy decision lacked clarity on the limitations and the extent of safeguards under US law. In particular, the Working Party was concerned that US law (and practice) did not exclude the possibility of mass, indiscriminate data collection; and that the role of the proposed Privacy Shield Ombudsperson was not spelt out in sufficient detail.[108] In particular, the Working Party considered that the powers and position of the Ombudsperson needed to be clarified to demonstrate that the role was truly independent and capable of offering effective remedies. Given that these issues are central to any assessment of the extent to which the Privacy Shield complies with the CJEU's ruling in *Schrems*, including the analysis of proportionality, this section of the Working Party's analysis is expanded upon immediately below. Finally, the Working Party welcomed the ongoing annual joint review process for the Privacy Shield, but recommended clarification and agreement on the elements to be included in the joint reviews.[109]

---

the Rules of Procedure, 24 May 2016. Subsequently, on 30 May 2016, the European Data Protection Supervisor released an opinion on the Privacy Shield draft adequacy decision which expressed very similar concerns to those set out in the Working Party's opinion: European Data Protection Supervisor, *Opinion on the EU-U.S. Privacy Shield draft adequacy decision*, Opinion 4/2016, 30 May 2016.

106 Article 29 Data Protection Working Party, *Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision*, 16/EN WP 238, Adopted on 13 April 2016, pp. 12–14.

107 Ibid. pp. 17–18.

108 Ibid., pp. 51–52.

109 Ibid., p. 58.

As explained above, on the analysis presented in this chapter, in *Schrems* the CJEU found that the Safe Harbour Agreement was invalid mainly on the basis that the broad derogation for national security, public interest and law enforcement requirements in Annex I to the Commission decision, which allowed for bulk collection and access to personal data by US public authorities, was disproportionate to the legitimate objectives of national security and law enforcement. This conclusion was reinforced by a lack of enforceable remedies, and absence of procedural safeguards, for EU data subjects in relation to the actions of US public authorities. It is therefore unsurprising that the most significant weaknesses with the Privacy Shield draft decision identified by the Working Party concern the extent to which the derogations for US public authorities in Annex II to the draft decision fail to comply with EU jurisprudence relating to the protection of fundamental rights.

In undertaking this analysis, the Working Party adopted a framework which it set out in a working document on the justification of interferences with the rights to privacy and data privacy through surveillance measures, especially in the context of data transfers to the US, which it published contemporaneously with its Privacy Shield opinion.[110] Given the policy orientation of the Working Party's analysis, its approach to justifications for interferences with privacy rights is unsurprisingly more structured and complete than that applied by the CJEU in invalidating the Safe Harbour Agreement in *Schrems*. Drawing on the human rights jurisprudence of both the Strasbourg and Luxembourg courts, the working document formulated the following four European Essential Guarantees, which must be in place if interferences to fundamental rights are to be justifiable:

A. Processing should be in accordance with the law and based on clear, precise an accessible rules.
B. Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated.
C. An independent oversight mechanism should exist, which is both effective and impartial.
D. Effective remedies need to be available to the individual.[111]

Regarding Guarantee A, which essentially relates to the foreseeability of lawful interferences as a means of protection against arbitrariness, the Working Party

110 Article 29 Data Protection Working Party, *Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring data (European Essential Guarantees)*, 16/EN WP 237, Adopted on 13 April 2016.

111 Article 29 Data Protection Working Party, *Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision*, 16/EN WP 238, Adopted on 13 April 2016, pp. 11–12.

noted the significant improvements in the transparency of US public intelligence activities since the Snowden revelations, including information published in relevant PCLOB reports and limitations introduced by PPD-28. Nevertheless, especially in light of remaining uncertainties concerning the operation of EO-112333, the Working Party concluded that, without further clarification, it was impossible to determine whether the US regime was sufficiently foreseeable.[112]

On the analysis presented in this chapter, the availability of procedural safeguards, including effective remedies, is relevant to the proportionality assessment; it is therefore appropriate to consider Guarantees B to D together. One possible reading of the *Schrems* ruling is that, building on *Digital Rights Ireland*, the CJEU effectively concluded that bulk collection of personal data by US intelligence agencies can never be proportionate. Nevertheless, as pointed out by the Working Party in its working document on justifications, to date neither the Strasbourg nor the Luxembourg courts appear to have adopted a final position on whether or not bulk collection can ever be justifiable, with some clarification on this issue expected from the forthcoming CJEU decisions referred to earlier in this chapter.[113] That said, and while noting that the application of proportionality to this area may be qualified or revised by the CJEU in the impending decisions, the Working Party reiterated its consistent conclusion that 'massive and indiscriminate collection of data (non-targeted bulk collection) in any case cannot be considered proportionate'.[114] This means that the extent to which collection of data by intelligence agencies is targeted so as to be related to legitimate national security objectives must be absolutely central to the proportionality analysis, especially where communications content is collected.

As explained above, since the Snowden revelations, the US government has taken steps to ensure that intelligence gathering is less indiscriminate, including the injunction in PPD-28 that collection of personal data must always be 'as tailored as feasible'. Nevertheless, as made clear in the ODNI letter annexed to the Commission's draft adequacy decision, the US continues to reserve the right to engage in bulk collection of signals intelligence where necessary. As, according to publicly available information, US intelligence agencies continue to engage in bulk, indiscriminate collection, or at least refuse to exclude doing so, the Working Party reached the inevitable conclusion that the Privacy Shield,

112 Ibid., p. 37.

113 Article 29 Data Protection Working Party, *Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring data (European Essential Guarantees)*, 16/EN WP 237, Adopted on 13 April 2016, p. 8.

114 Ibid., p. 12.

by not ruling this out, allowed a disproportionate interference with rights.[115] Above and beyond this, the Working Party expressed concerns that the broad assurance that data collection would be 'as tailored as feasible' could still allow for massive data collection, which might also fail the proportionality test.[116] Accordingly, the Working Party, at a minimum, required further information on mass collection practices by US intelligence agencies before a final conclusion on adequacy could be reached.

Regarding the need for effective and independent oversight, the Working Party noted the substantial internal oversight mechanisms in place in the US, but pointed out that effective oversight depends on an independent, external body. As there is no oversight whatsoever of surveillance programmes undertaken pursuant to EO-12333, Guarantee C could hardly be satisfied in relation to these programmes. Moreover, the regime administered by the FISA Court provides no effective oversight for non-US persons.[117]

As explained earlier in this chapter, in the *Schrems* ruling, the CJEU identified the absence of any effective legal remedies against US public authorities as an important weakness in the Safe Harbour Agreement, and also found that the lack of legal recourse against state intrusions compromised Art. 47 of the Charter. Significant elements of the Privacy Shield are aimed at improving the legal recourse mechanisms available to EU persons. In relation to the activities of US public authorities, the main new recourse avenue is the proposal to create a Privacy Shield Ombudsperson, to receive and respond to individual complaints. While welcoming the introduction of this new recourse mechanism, the Working Party concluded that the Privacy Shield failed to specify the powers and position of the Ombudsperson with sufficient detail, leaving doubts regarding its independence from government, the extent of its investigatory powers, its remedial powers, and the absence of an appeals process.[118] As explained above, according to the Working Party, the two major factors compromising the adequacy of the Commission's draft decision are the failure of the Privacy Shield to exclude untargeted mass collection of data by US security agencies and the lack of clarity regarding the role and powers of the Ombudsperson. Both of these shortcomings arise from the disproportionality of the US legal and administrative regimes that apply to the collection and analysis of data by security agencies, and especially the regime that applies to the data of non-US persons.

---

115 Article 29 Data Protection Working Party, *Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision*, 16/EN WP 238, Adopted on 13 April 2016, p. 40.

116 Ibid., p. 40.

117 Ibid., pp. 42–43.

118 Ibid., pp. 49–51.

The Privacy Shield, as a negotiated international agreement, necessarily embodied compromises between the parties. It is clear that both parties to the negotiation, the US Department of Commerce and the European Commission, share interests in ensuring the continued viability of trans-Atlantic data transfers while insulating the agreement against the potential for an adverse CJEU ruling. The negotiations took place in the shadow of considerable uncertainties in the CJEU's application of the proportionality principle to mass data collection, including uncertainties arising from the rulings in *Digital Rights Ireland* and *Schrems*, and including whether or not bulk collection by security agencies can ever be proportionate. These uncertainties enabled the negotiators to conclude that a regime in which some form of bulk collection by security agencies is restricted, but not ruled out could, nevertheless, be adequate. The Commission also concluded that the Privacy Shield Ombudsperson mechanism provided sufficient safeguards for EU data subjects, including by receiving individual complaints and investigating compliance with US law. Nevertheless, the agreement and the Commission's draft decision cannot disguise the hallmarks of haste. On the basis of the CJEU's ruling in *Schrems*, the Working Party's conclusions that more information on US mass data collection practices and on the details of the ombudsperson mechanism is needed before an adequacy decision can be made must surely be correct. But, that said, as argued in this chapter, gaps and ambiguities in the CJEU's proportionality analysis mean that precisely what changes might be required for the agreement to be adequate, including whether the US must undertake to engage only in targeted data collection, is necessarily uncertain; and may require further rulings by the CJEU, some of which are forthcoming, to be clarified.

10. CONCLUSION

In Europe, proportionality has emerged as a meta-principle which, among other things, is the key legal standard for establishing the balance between the protection of rights, on the one hand, and public policies, on the other. Thus, it is unsurprising that the principle, as applied by the CJEU, has played the central role in establishing the balance between state surveillance and the rights to privacy and data privacy in cases such as *Digital Rights Ireland*, but also, as argued in this chapter, underpins the *Schrems* ruling. As illustrated by these cases, under the influence of the EU Charter, the Court has taken an increasingly expansive approach to the protection of privacy and data privacy, according less deference to EU policy-making institutions. This is clearly reflected in the level of scrutiny applied to interferences with these rights, which under proportionality analysis now requires a form of strict review. While a degree of flexibility and sensitivity to the facts of instant cases must be retained by courts applying the proportionality principle this should not, however, be at the expense of properly

constrained judicial decision-making. Applying a rigorous approach to the application of the proportionality principle is essential if courts are to escape charges of arbitrarily substituting their judgments for those of policy-making institutions, and for the promotion of greater certainty and predictability. Yet, as this chapter has explained, the jurisprudence of the CJEU, culminating in the *Digital Rights Ireland* and *Schrems* rulings, has given rise to significant legal uncertainties, including in relation to the standard and intensity of review of measures that may interfere with the rights to privacy and data privacy and, from a policy-making perspective, creating much uncertainty about whether bulk data collection is ever permissible.

Despite weaknesses with the CJEU's approach to proportionality, this chapter contends that the principle is the correct legal framework for evaluating infringements of fundamental rights, including the rights to privacy and data privacy. This is because, applying a rights-based perspective, the principle ensures that the courts ask the right questions. While rights sceptics contend that rights-based judicial review, such as that undertaken in jurisdictions with a 'thick' concept of the rule of law, is somehow antithetical to democracy, the appropriate protection of rights is a pre-condition to sustainable democratic polities. This is especially the case where democratic processes are incapable of effectively limiting state-based intrusions, which appears to be the case with the apparently inexorable drive to broader and more intensive surveillance practices by state intelligence agencies. In this context, an appropriately defined proportionality principle may well be the main legal bulwark against privacy and democracy-corrosive practices.

While mass indiscriminate surveillance, with no adequate procedural safeguards, would fall foul of any rights-based review, extra-territorial surveillance by state-based agencies may escape review in jurisdictions where rights are not extended to foreigners. Under EU law, the requirement that transborder transfers of personal data should be permissible only where a third country provides adequate protection is a mechanism for ensuring transborder protection of the rights of EU data subjects. Nevertheless, the need for a single jurisdiction, such as the EU, to establish such a mechanism, reflects a significant limitation of the international human rights framework. In an era of ubiquitous transborder transfers of personal data, where rights can be readily invaded at a distance, the proper protection of rights must entail limitations on extra-territorial interferences by state parties. The proportionality principle, appropriately defined and rigorously applied, is an eminently suitable legal rubric for evaluating the extra-territorial surveillance practices of state agencies.

The current process of revising the data transfer arrangements between the EU and the US, in the shadow of the *Schrems* ruling, therefore represents a highly significant test of the principles that should apply to transborder data surveillance practices. As explained in this chapter, however, uncertainties in the EU rights-based framework, and especially in the content and application of the

proportionality principle, have complicated the process for finalising a US-EU framework to replace the invalidated Safe Harbour Agreement. The uncertain jurisprudence has, in particular, created wriggle room for the European Commission to conclude, in its February 2016 draft decision on the Privacy Shield, that a US regime that fails to sufficiently exclude the possibility of bulk data collection, and includes scant details on the key ombudsperson recourse mechanism, nevertheless confers the required high level of protection of the rights to privacy and data privacy of EU data subjects. Yet, the Article 29 Working Party was surely correct to express serious concerns that, at a minimum, without further details concerning US bulk collection practices and the ombudsperson mechanism, it would be imprudent to conclude that the Privacy Shield agreement confers adequate protection. At the time of writing this chapter, the position was further complicated by the prospect of two impending, and likely highly relevant, CJEU rulings on the critical issue of bulk data collection. These two related pending developments – the process for adjusting the Privacy Shield agreement so that it is able to comply with EU law and the forthcoming CJEU rulings – seem likely to set the framework establishing the permissible limits on state based surveillance, especially in the trans-Atlantic context, for some time to come. As this chapter argues, the development of a clearer, more rigorously elaborated proportionality principle by the CJEU would serve both to better protect the rights of EU data subjects and add much-needed commercial and political certainty.