CENTRO STUDI SUL FEDERALISMO

ISTITUTO DI DIRITTO, POLITICA E SVILUPPO
Scuola Superiore Sant'Anna

SURVEILLANCE, PRIVACY AND TRANSATLANTIC RELATIONS. CONCLUDING REMARKS

PETER HUSTINX

CENTRO STUDI SUL FEDERALISMO

Via Real Collegio, 30
10024 Moncalieri (TO)

www.csfederalismo.it
info@csfederalismo.it

SCUOLA SUPERIORE SANT'ANNA

Istituto DIRPOLIS
Piazza Martiri della Libertà 33
56127 Pisa

www.santannapisa.it/it/istituto/dirpolis/istituto-dirpolis
dirpolis@santannapisa.it

SURVEILLANCE, PRIVACY AND TRANSATLANTIC RELATIONS

Concluding Remarks

Peter Hustinx[1]*

1. Introduction

In March 2015, three keynote speakers addressed a record size audience of about 3000 privacy professionals at the IAPP Global Privacy Summit, only a few blocks from the White House in Washington DC.[2] The first one was Glenn Greenwald, the Pulitzer Prize winning journalist who first interviewed Edward Snowden and played a key role in the subsequent news reports in the *Guardian* and the *Washington Post*.[3] He addressed two questions: 1) how was it to meet Edward Snowden, and 2) what has changed since? His answer to this second, more relevant, question was, put very briefly: at first sight not a great deal, but at further analysis quite a lot. Two aspects of this deeper change are that issues relating to surveillance are now much more the subject of public debate, and the role of the privacy profession in addressing them has become much more obvious.[4] The second keynote speaker was Michael Sandel, a political philosopher from Harvard with a special reputation in ethical dilemmas.[5] He animated a fascinating Socratic debate with the vast audience on 'why privacy matters'. The third keynote speaker was an historian and curator, Sarah Lewis, who gave a clear answer on this topic from her perspective: privacy is an essential ingredient of creativity and innovation, and she mentioned a series of success stories that were born out of failure.[6]

---

[1] Former European Data Protection Supervisor (2004-2014). This work is forthcoming as the concluding chapter in: David Cole, Federico Fabbrini and Stephen Schulhofer (eds), *Surveillance, Privacy and Transatlantic Relations* (Oxford, Hart Publishing, 2016)

[2] The International Association of Privacy Professionals (IAPP) was established in 2003 and now has about 25.000 members of which 3000 in Europe. Membership worldwide grew in 2015 with 19% and in Europe even with 30%. The Global Privacy Summit in Washington DC is the annual top event, with other events taking place at various locations in the world throughout the year. The author has been on the IAPP Board of Directors since early 2015.

[3] See also Glenn Greenwald, *No place to Hide: Edward Snowden, the NSA and the US Surveillance State*, New York, 2014.

[4] The full text of Greenwald's keynote is still available at https://iapp.org/news/a/glenn-greenwald-the-full-keynote-address. See also *Greenwald's Call to Privacy Pros: Subverting Injustice Rests on Your Shoulders*, The Privacy Advisor, March 5, 2015.

[5] See e.g. Michael J. Sandel, *Justice; What's the right thing to do?* New York, 2009, and Michael J. Sandel, *What Money Can't Buy; The Moral Limits of Markets*, New York, 2012.

[6] See *Privacy: An Essential Ingredient in Failure and Success*, The Privacy Advisor, March 9, 2015, with examples ranging from Martin Luther King to Harry Potter author J.K. Rowling.

2. Lessons learned

There is no doubt that privacy has emerged as a hot subject in recent years. To a large extent this is due to the Snowden revelations. However, further developing a theme touched on by Greenwald, the question should be asked: what have we learned since? Here we can see a broad landscape with different layers. First, the breathtaking scale and far reaching impact of the Digital Society can no longer be ignored, but also the vulnerability of our digital environment has now become evident. Second, we have now seen many illustrations of the vast impact of unlimited mass surveillance. Third, the complicity of different well known Internet giants – active or passive – in wide ranging surveillance by the state has become abundantly clear. Fourth, we should finally also take a careful look at our Internet infrastructure and admit that it was not only used to facilitate – lawful or unlawful – state surveillance. Most successful business cases on the Internet – involving 'free services' in exchange for profitable advertising – are still largely based on virtually unlimited surveillance by private actors. This is why some experts argue that the Internet itself has developed into an instrument of surveillance.[7]

This dubious mix of factors has contributed to an increase in political attention for privacy and data protection in many parts of the world and to their reaffirmation as corner stones of a democratic society based on the rule of law.[8] In Europe this has resulted in an approach at different levels and with different means, but with a strong emphasis on both public and private organisations that are involved in the processing of personal information, without necessarily being engaged in any kind of mass surveillance. Those that are involved in surveillance, receive special attention under a different heading. Any connections between these different worlds also receive special attention. This makes great practical sense and has so far led to good results.

3. The EU Charter of Fundamental Rights

The strongest reaffirmation of privacy and data protection in the EU took place at the end of 2009 when – due to the entering into force of the Lisbon Treaty – the EU Charter of Fundamental Rights became directly binding, not only for the EU institutions and bodies, but also for the Member States

[7] Bruce Schneier, *Data and Goliath; The Hidden Battles to Collect Your Data and Control Your World*, New York, London, 2015.

[8] In the European Parliament, in spite of heavy lobbying by industry and vested interests, these factors have no doubt galvanized a large majority in support of the Data Protection Reform package (see infra points 8 and 9).

when acting within the scope of EU law.[9] Articles 7 and 8 of the Charter lay down separate rights to the respect for private and family life, and to the protection of personal data. A few years later, the European Court of Justice ruled that the Charter *always* applies when a Member State acts within the scope of EU law.[10] In addition, Article 16(2) of the Treaty on the Functioning of the European Union (TFEU) provides that the European legislature shall lay down rules on the protection of individuals with regard to the processing of personal data, thus providing a mandatory basis for a wide ranging review of the existing legal framework on data protection.[11]

The inclusion of privacy and data protection in two separate articles did not happen by accident. The distinction in the Charter between the right to the respect for private and family life in Article 7 and the right to the protection of personal data in Article 8 could build on a legal development of several decades. Although these provisions are closely related, they also have a different character that should not be overlooked. The first one deals with a classic fundamental right – providing legal protection against *interference* – while the second one has been conceived as a positive right to be protected according to certain conditions and standards.[12]

4. Respect for private life

The concept of a 'right to privacy' emerged in international law first in a rather weak version in Article 12 of the Universal Declaration of Human Rights[13], according to which no one shall be subjected to *arbitrary* interference with his privacy, family, home or correspondence. A more substantive protection followed soon in Article 8 of the European Convention on Human Rights (ECHR)[14], according to which everyone has the right to *respect* for his private and family life, his home and his correspondence, and no interference by a public authority with the exercise of this right is allowed except in accordance with the law and where necessary in a democratic society for certain important and legitimate interests.

[9] The Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, entered into force on 1 December 2009. Article 6(1) of the TEU now provides that the Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, "which shall have the same legal value as the Treaties".
[10] Case C-617/10, *Åkerberg Fransson*, and Case C-399/11, *Melloni*, both 26 February 2013
[11] The entering into force of the Treaty coincided with the start of a new Commission mandate. Vice-President Viviane Reding made the Data Protection Reform one of her top priorities.
[12] See Peter Hustinx, *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation* in: Collected Courses of the European University Institute's Academy of European Law, 24th Session on European Union Law, 1-12 July 2013.
[13] UN General Assembly, Paris 1948
[14] Council of Europe, Rome 1950

According to the case law of the European Court of Human Rights, the scope of Article 8 is not limited to 'intimate' situations, but also covers certain aspects of professional life and behaviour in public.[15] On the other hand, those cases often concern specific situations, which involve sensitive information (medical or social services), justified expectations of privacy (confidential use of telephone or email at work) or inquiries by police or secret services. The Court has so far never ruled that *any* processing of personal data - *regardless* of its nature or context - falls within the scope of Article 8. This provision now fully corresponds with Article 7 of the Charter.

5. Protection of personal data

The concept of 'data protection' has a different genesis. In the early 1970s the Council of Europe concluded that Article 8 ECHR had a number of shortcomings in the light of recent developments, particularly the use of information technology: the uncertain scope of 'private life' under Article 8 ECHR, the emphasis on protection against interference by 'public authorities', and the lack of a pro-active approach, also dealing with the possible misuse of personal information by companies or other relevant organisations in the private sector.[16]

This resulted in the adoption in 1981 of the Data Protection Convention, also known as Convention 108[17], which has now been ratified by 47 countries, including all EU Member States, most Member States of the Council of Europe and one non-European State.[18] The purpose of the Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ('data protection').[19] The concept of 'personal data' has been defined as 'any information relating to an identified or identifiable individual ('data subject')'.[20]

[15] See e.g. *Klass v Germany*, ECHR (1978), A-28; *Malone v United Kingdom*, ECHR (1984), A-82; *Leander v Sweden*, ECHR (1987), A-116; *Gaskin v United Kingdom*, ECHR (1989), A-160; *Niemietz v Germany*, ECHR (1992), A-251-B; *Halford v United Kingdom*, ECHR 1997-IV; *Amann v Switzerland*, ECHR 2000-II, and *Rotaru v Romania*, ECHR 2000-V.
[16] Explanatory Report to Convention 108 (see footnote 16), para. 4
[17] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, ETS 108.
[18] Uruguay was the first non-European State to ratify the Convention in April 2013.
[19] Article 1
[20] Article 2 sub a

The main EU instrument on the subject so far, Directive 95/46/EC,[21] took Convention 108 as a starting point and further developed and specified it in different ways. This basically amounted to a system of 'checks and balances' with substantive principles, rights for data subjects, obligations for responsible organisations and oversight by an independent authority.[22] These main elements of the protection of personal data are now also visible in Article 8(2) and (3) of the Charter.[23]

6. National security

The above provisions of EU law do not apply to the national security of EU Member States. According to Article 4(2) TEU, this is an "essential function" of the Member States, which remains their "sole responsibility".[24] However, the national security of third countries is not covered by this exemption. Moreover, the exclusion of Member States' national security from the scope of EU law does not mean that this remains an unregulated area, in particular as regards the protection of fundamental rights: the Council of Europe instruments mentioned above and national laws are in most situations fully applicable to this field.

In particular, the ECHR and Convention 108 apply to many of the relevant processing operations by member states as the general application to most of their parties does not exclude national security as a whole.[25] These instruments also create a positive obligation for the parties to secure privacy and data protection rights to everyone within their jurisdiction and to adopt domestic law giving effect to data protection principles.[26]

Where the above mentioned EU and Council of Europe instruments apply, the rights to privacy and data protection can be restricted if necessary to safeguard national security or state security, among

[21] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).
[22] See Hustinx (footnote 11).
[23] Article 8(2): "Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified." Article 8(3): "Compliance with these rules shall be subject to control by an independent Authority."
[24] Article 4(2) : "The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State."
[25] Only a minority of the parties to Convention 108 have deposited declarations in accordance with Article 3(2)(a) stating that the Convention will not apply to "automated personal data files" relating to "state security" or "state secrets".
[26] See Articles 1 and 8 of the ECHR and Article 4(1) of Convention 108. See also *von Hannover v Germany*, ECHR 2004-VI, and *K.U. v Finland*, Application 2872/02, ECHR 2008-V.

other reasons.[27] However, such limitations have to be applied in a restrictive way, and any limitation to the rights granted can only be allowed if laid down by a foreseeable and accessible law and only if necessary in a democratic society.[28] The exceptions provided by these instruments for national security purposes cannot justify massive limitations, for purposes which go beyond what is strictly necessary to safeguard national security.

7. Enforceability

National laws implementing Directive 95/46/EC are applicable to processing operations in the context of the activities of an establishment of controllers in the EU.[29] They are also applicable where a non EU controller is established in a place where a Member State's national law applies by virtue of international law, or if the responsible controller is using equipment in the EU.[30] In these cases, EU Data Protection Authorities have thus competence to directly enforce their national data protection laws against organisations that have provided access to or disclosed personal data to any government agency in breach of national data protection laws.

Articles 1 and 8 of the ECHR create - as just mentioned - a positive obligation for Parties to the Convention to protect privacy and data protection rights. In cases of unlawful or excessive surveillance, or complicity of private organisations in such activities, this obligation has not been fulfilled. Convention 108, which applies to processing operations in the States party to that Convention, both in the public and in the private sector, has in that situation not been respected either. EU Member States and any other Party to the ECHR can be brought in front of the European Court of Human Rights for not complying with their obligation to "secure to everyone within their jurisdiction the rights and freedoms provided in the Convention."[31]

8. Need for more effectiveness

Although all these arrangements have now been in place for a while, there is still the need for greater effectiveness of applicable safeguards in practice. This is mostly for two reasons: first, the main legal instrument for data protection, Directive 95/46/EC, was adopted when the Internet was

[27] See e.g. Article 8(2) of the ECHR, Article 9(2)(a) of Convention 108 and Articles 9(2)(a) and 13(1)(a) of Directive 95/46/EC.
[28] See e.g. *Klass v Germany*, ECHR (1978), A-28, and CJEU in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger*, 8 April 2014.
[29] See Article 4(1)(a) of Directive 95/46/EC.
[30] See Article 4(1)b) and (c) of Directive 95/46/EC.
[31] See Article 1 of the ECHR

still in its infancy and mobile applications were completely unknown. Second, current legal arrangements are too often only "law on the books" and not enough "law on the ground."[32] Moreover, the implementation of Directive 95/46/EC in presently 28 national laws has resulted in too much legal diversity and complexity. This has also worked to erode the effectiveness of current data protection laws in a cross-border or EU-wide context.

This is why the EU data protection reform set in motion in 2009 was designed to ensure stronger and more effective protection of data subjects and more consistency across the European Union. In January 2012, the European Commission presented a package of proposals in order to update and modernise the present EU legal framework.[33] This package has since then been the subject of very intense discussions, both inside and outside the European Parliament and the Council, and resulted in a political agreement between the two legislative branches, likely to be confirmed and finalised by the spring of 2016.[34] Although these efforts did not address surveillance for national security purposes *per se*, they will undoubtedly have an indirect effect on it, since the new arrangements will apply, probably as from spring 2018, to all companies active in the EU, regardless of the location from where they are operating.[35]

9. Rebuilding Trust in EU-US Data Flows

In November 2013, a few months after the first Snowden revelations, the Commission adopted two relevant communications: one focused on the functioning of the Safe Harbour arrangement for data flows between the EU and US, and another reflected more in general on the political situation.[36]

[32] See Kenneth Bamberger and Deirdre Mulligan, *Privacy on the Books and on the Ground*, Stanford Law Review 63, no. 2 (2011), p. 247-316, and *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*, Cambridge, London, 2015.

[33] See Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: "Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century", COM (2012) 9 final.

[34] See Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), and Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (both published on 15 December 2015).

[35] According to its Article 4(2), the new Regulation will also apply to companies which are not established in the EU, but offer goods or services to data subjects in the EU or monitor their behaviour in the EU.

[36] See Communication from the Commission to the European Parliament and the Council on "Rebuilding Trust in EU-US Data Flows", COM(2013) 846 final, and Communication from the Commission 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.

The European Data Protection Supervisor (EDPS) issued a formal Opinion with comments on both communications, and more specifically on eight future steps to be taken.[37]

Data protection reform

The first point raised by the EDPS was the need for a swift adoption of the EU data protection reform.[38] In this context, this involved in particular the extension of the territorial scope of application of EU rules, the clarification of the conditions for transfers of personal data to third countries, the harmonisation and reinforcement of the enforcement powers of EU Data Protection Authorities, the inclusion of clear rules on the obligations and liabilities of controllers and processors, and the establishment of comprehensive rules for the protection of personal data in the law enforcement area.

The EDPS also emphasized the need for adequate protection of commercial data in the case of their further use for law enforcement purposes and clear rules on international conflicts of jurisdiction. The first issue may arise where personal data initially subject to the proposed Regulation – e.g. at a bank or air carrier – are subsequently processed for purposes of law enforcement and by authorities subject to the proposed Directive. This issue has not been solved entirely, also due to the fact that national laws implementing the Directive may take different positions. The second issue has been addressed in a provision in the proposed Regulation on transfers or disclosures to third countries not authorised by EU law.[39]

Safe Harbour

The second point was the need to strengthen the Safe Harbour along the lines proposed at the time by the Commission.[40] The EDPS would have preferred the use of more affirmative language and stricter deadlines in addressing the deficiencies already previously identified in the scheme. On the basis of the outcome of a review, different scenarios could be envisaged, including suspension or revocation of the Safe Harbor arrangement, where necessary.

[37] EDPS Opinion of 20 February 2014 on the Communication from the Commission to the European Parliament and the Council on "Rebuilding Trust in EU-US Data Flows", and the Communication from the Commission 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", available at www.edps.europa.eu.

[38] Ibid, at 40-44.

[39] Article 43a will now read: "Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to [Chapter V]." This may help to prevent unlawful disclosures and points the way to diplomatic solutions of any conflicts of jurisdiction.

[40] EDPS Opinion, at 45-52.

On 6 October 2015, the European Court of Justice invalidated the Commission's Decision 2000/520 finding that the Safe Harbour arrangement provided an adequate level of protection under Article 25 of Directive 95/46/EC.[41] Since then the Commission and the US Government have stepped up their efforts to conclude a new arrangement, without the deficiencies identified before. The most difficult issues seem to relate to the need for better assurances against excessive surveillance. We will return to this subject at the end.[42]

EU-US law enforcement cooperation

The third point was the need to strengthen data protection safeguards in EU-US law enforcement cooperation.[43] Current negotiations on an "umbrella agreement" should according to the EDPS not legitimize massive data transfers of data, but comply with the existing data protection framework and with the outcome of its current review process. In particular, effective redress mechanisms should be accessible to all data subjects, regardless of their nationality. This should in due course also apply to existing international agreements, where necessary on the basis of appropriate transition clauses.

In September 2015, the Commission announced that negotiations for an EU-US data protection "Umbrella Agreement" for EU-US law enforcement cooperation were finalized and the agreement had been reached. However, the agreement would be signed and formally concluded only after the US Judicial Redress Bill, granting judicial redress rights to EU citizens, and presently still pending before the US Congress, had been adopted.[44]

US reform process

The fourth point was the need to address European concerns in the ongoing US reform process.[45] According to the EDPS, the Commission should support efforts by the US Administration and US Congress to enact a general privacy act with strong safeguards and adequate oversight, in particular in areas where any substantial protection of privacy is currently lacking.

In February 2012, President Obama published a white paper with a blueprint for comprehensive privacy safeguards for consumers online.[46] In February 2015, this was followed by the presentation

[41] Case C-362/14, *Maximilian Schrems v Data Protection Commissioner*, 6 October 2015.
[42] See infra, point 10.
[43] EDPS Opinion, at 53-60.
[44] Questions and Answers on the EU-US data protection "Umbrella Agreement" (MEMO/15/5612)
[45] EDPS Opinion, at 61-66.
[46] *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, White House, February 2012.

of a preliminary draft for a Consumer Privacy Bill of Rights Act.[47] Any further legislative efforts along these lines have so far failed. However, the Federal Trade Commission has gradually emerged as the leading privacy regulator in the US, mainly exercising its general authorities on the basis of the FTC Act of 1914 against unfair and deceptive trade practices.

Transatlantic trade

The fifth point concerned the ongoing negotiations between the EU and the US on a Transatlantic Trade and Investment Partnership (TTIP).[48] These negotiations should according to the EDPS not have an adverse impact on the protection of personal data of citizens. At the same time, the Commission should consider setting a common goal of gradual development towards greater interoperability of legal frameworks for privacy and data protection. At the time of writing, the negotiations are still ongoing.

International privacy standards

The sixth point raised in the EDPS Opinion was the need to promote privacy standards internationally.[49] In his view, this international promotion of privacy standards should include: promoting full consistency of any new international instruments with the EU data protection framework; promoting the adhesion of third countries, and in particular the US, to Council of Europe Convention 108; and supporting the adoption of an international instrument – e.g. at UN level on the basis of Article 17 of the International Covenant on Civil and Political Rights (ICCPR) – requiring the respect of privacy and data protection standards by intelligence activities.[50]

Intelligence activities

The seventh point was the need to subject intelligence activities to appropriate safeguards.[51] The EDPS argued that surveillance activities should at all times be obliged to respect the rule of law and the principles of necessity and proportionality in a democratic society. Legal frameworks at relevant levels should therefore be clarified and where necessary supplemented. These frameworks should include appropriate and sufficiently strong oversight mechanisms.

[47] Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015, February 2015
[48] EDPS Opinion, at 67-69.
[49] EDPS Opinion, at 70-73.
[50] Initiatives by Germany and France to find a bilateral arrangement with the US have not succeeded so far. Initiatives in the UN by Germany and Brazil and others have *inter alia* led to the appointment of a Special Rapporteur on the right to privacy (see: http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx).
[51] EDPS Opinion, at 74-76.

Effective IT security

The eighth point was the need to ensure effective IT security.[52] The EDPS pointed out that EU institutions and all relevant entities in the Member States are as controllers also directly responsible for ensuring effective IT security. This involves carrying out a data security risk assessment at the appropriate level. It also requires encouraging research on encryption mechanisms and raising data controllers and citizens' awareness on privacy risks of the products sold or used, and requiring that developers use concrete design methods to avoid or at least reduce these risks.[53]

10. The CJEU decision in *Schrems*

We will conclude these remarks with a few observations on the CJEU's decision in *Schrems.*[54] The Safe Harbour arrangement has been controversial since its start in 2000. While the criticism focused initially on the substance of the arrangement and later on the way it was implemented in practice, since the Snowden revelations Safe Harbour was more and more perceived as a facilitator of data transfers subject to US surveillance.[55] The Commission's strategy has been to strengthen the Safe Harbour on a number of points, including those defining the scope of possible exceptions for lawful access or onward transfers. The Court's invalidation of the Commission's initial decision on Safe Harbour allowed all different opponents to claim victory and to agree on the practical outcome of the case.

However, the subtlety of the Court's decision has not been noticed by everyone. For one thing, the Court has not directly evaluated US law – either in general or on surveillance in particular – and not even evaluated the general merits of the Safe Harbour arrangement.[56] Instead, it has almost entirely concentrated on the role of the Commission in finding adequacy - in terms of what it did or not do in 2000, and what it should have done and should do at any point in the future. Moreover, in that context, the Court was legally bound to respect the findings of the referring Irish Court.

---

[52] EDPS Opinion, at 77-78.

[53] The EDPS has also established an Internet Privacy Engineering Network (IPEN) with the purpose "to bring together developers and data protection experts with a technical background from different areas in order to launch and support projects that build privacy into everyday tools and develop new tools which can effectively protect and enhance our privacy" (see: https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/IPEN).

[54] See footnote 40. The first question in the case, i.e. whether the Irish DPA had the power to investigate Mr Schrems' complaint, will remain untouched.

[55] The word "safe" in Safe Harbor – initially only used as a shelter against regulatory action – turned into a misleading term after revelations that some or even much personal data had not been so safe after all. This in spite of the fact that the purpose of the arrangement had been much wider and the problem of lawful or unlawful surveillance was a general issue, also arising under other instruments for transborder data flow (such as model contracts and binding corporate rules) and in fact also under the EU framework itself.

[56] See the CJEU in *Schrems*, at 98: "Consequently, without there being any need to examine the content of the safe harbour principles, it is to be concluded ...".

As to the validity of Decision 2000/520, the Court basically found that the Commission had not respected the requirements stemming from Article 25(6) of Directive 95/46/EC, inter alia by only assessing the Safe Harbour arrangement itself and not whether US law in fact "ensures" adequate protection, and by applying the wrong standard: according to the Court, the Commission should not only have checked the "adequacy" but the "essential equivalence" of the protection under US law.[57] The Court also emphasized that the Commission's discretion in this assessment is reduced, with the result that its review of those requirements, read in the light of the Charter, should be strict.[58] This is evidence of the Charter's impact on the Commission's role, since the entry into force of the Lisbon Treaty in 2009.

The Court only went into the substance of the Safe Harbour arrangement in order to raise questions about the scope and the limits of the protection afforded by it under US law. These questions were all the more relevant, as the Commission had seriously criticized US practice along similar lines in its own communications. At the same time, the Commission's decision did not contain any finding as to the existence in the US of effective protection against interference with fundamental rights.[59] The Court also added a few observations about what could be expected from such protection under EU law.[60] These observations are no doubt very useful, but do not contain any direct findings on the quality of US law. In other words, they should mostly be regarded as important guidelines for the Commission.

It is also striking to see that the Court at different points seems to accept and even to emphasize the diversity of legal systems in the world. This is first implicit in the term "essential equivalence". A third country cannot be required to ensure an "identical" level of protection.[61] However, the Court adds two separate observations in order to further develop this idea. First, different means "must [...] prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the EU."[62] In other words: a functional requirement and an example of "principled pragmatism". Second, a system of self-certification – as in Safe Harbour – is not in itself unacceptable, but depends on the establishment of "effective detection and supervision mechanisms enabling any infringements […] to be identified and punished in practice."[63] Again,

[57] See *Schrems*, at 68-77 and 79-98
[58] See *Schrems*, at 78
[59] See *Schrems*, at 82-90
[60] See *Schrems*, at 91-95
[61] See *Schrems*, at 73
[62] See *Schrems*, at 74
[63] See *Schrems*, at 81

this is a Court speaking indirectly and very well aware of the stakes, both in general and in this particular case.

As a result, the Commission – and everyone else interested – is now much better informed about the requirements for an adequacy finding, both under the current Directive and the new Regulation.[64] The Commission will have to make a duly motivated finding that the third country in question ensures a level of protection that is essentially equivalent to that guaranteed in the EU under the current Directive or the new Regulation, read in the light of the Charter. Its discretion in reaching that result will be limited.

Whether the Commission and the US Government will be able to arrive at a "Safe Harbour 2.0" meeting that test, will mostly depend on the availability of effective assurances that any limitations or exceptions in such a scheme will not go beyond what is necessary in a democratic society for legitimate reasons, which must be subject to adequate legal safeguards and effective remedies in case of disputes. Other points on the EU list will be less controversial. However, it will also be important to see whether the US will ensure "effective detection and supervision mechanisms enabling any infringements […] to be identified and punished in practice". Moreover, further to the Court's emphasis on effective remedies, it will also be important to ensure that data subjects can exercise their rights of access and correction or deletion, including the right to judicial redress, in case of disputes with private parties in the US.[65]

If a Safe Harbour 2.0 is produced and the requirement of "essential equivalence" is met, that would not yet amount to a comprehensive Transatlantic Data Protection Framework for commercial data flows, as long as – what is likely – companies would still have the option to join it or not. Nor would it amount to an EU-US agreement on standards for "legitimate surveillance" or something similar. However, it would confirm once again that bridges can be built between the EU and the US, and it would set a benchmark for international relations in a wider context.[66]

[64] The Directive will continue to apply for two more years after the formal adoption of the new Regulation. The need for an "adequate level of protection" is maintained in the Regulation, but explained in more detail, both in Article 41(2) and recital 81, in the latter case with implicit reference to the CJEU: "[…] The third country should offer guarantees that ensure an adequate level of protection *essentially equivalent* to that guaranteed within the Union, [...]" [highlights added].

[65] It is likely that any "Safe Harbour 2.0" will be scrutinized and challenged in court, in which case the CJEU would be able to take a second look at the subject. Meanwhile, the next stages of the Schrems case in Ireland and similar cases before DPAs elsewhere may give rise to further case law about the same issues.

[66] The "Umbrella Agreement" for EU-US law enforcement cooperation mentioned above in point 9 – if finally concluded – might have a similar effect.