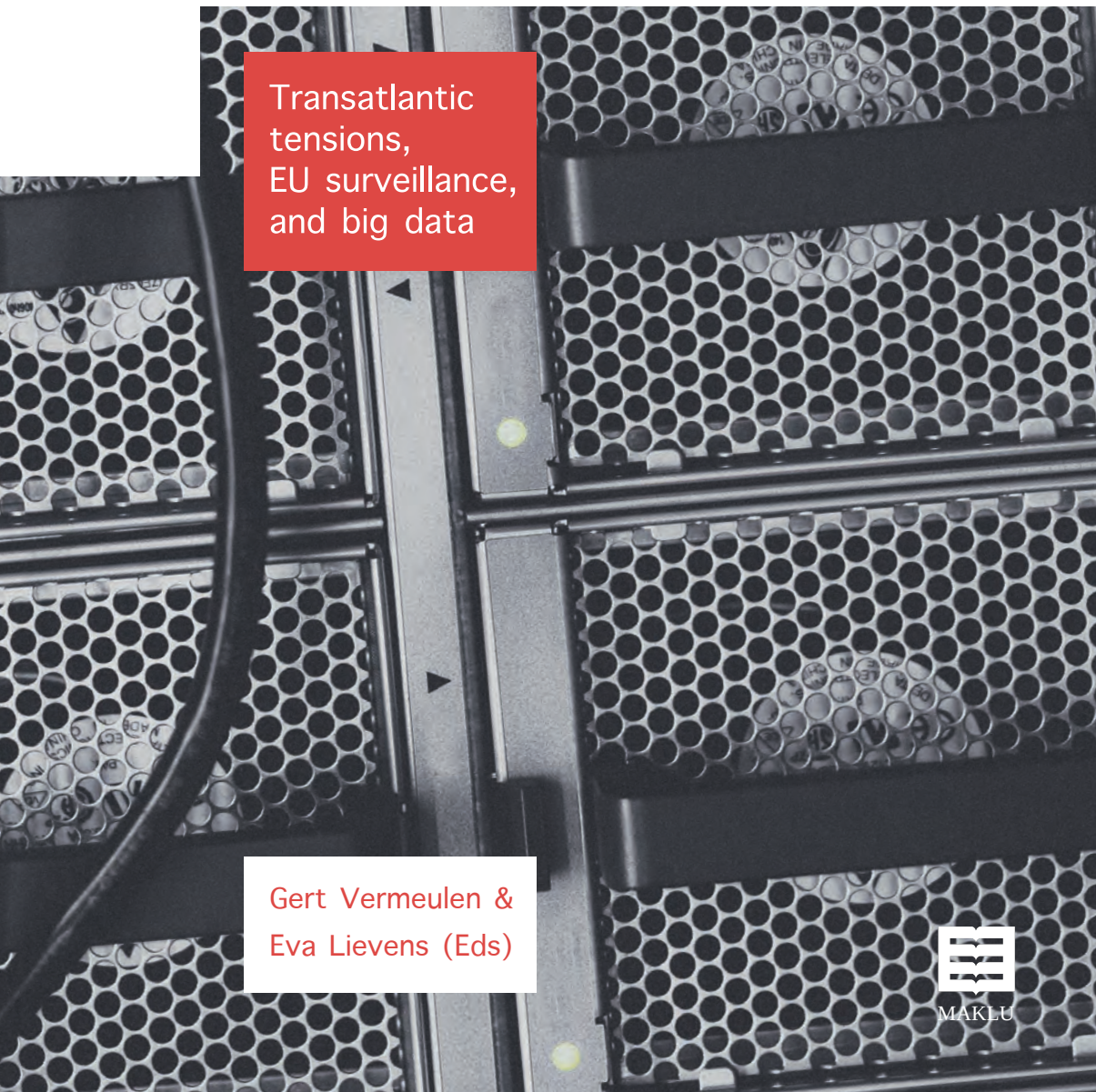
Data Protection and Privacy under Pressure



Transatlantic tensions, EU surveillance, and big data

Gert Vermeulen &
Eva Lievens (Eds)

MAKLU

Data Protection and Privacy under Pressure

Transatlantic tensions, EU surveillance, and big data

Gert Vermeulen
Eva Lievens
(Eds)

Maklu

Antwerp | Apeldoorn | Portland

Data Protection and Privacy under Pressure
Transatlantic tensions, EU surveillance, and big data
Gert Vermeulen and Eva Lievens (Eds)
Antwerp | Apeldoorn | Portland
Maklu
2017

341 p. – 24 x 16 cm
ISBN 978-90-466-0910-1
D/2017/1997/89
NUR 824

Maklu-Publishers
Somersstraat 13/15, 2018 Antwerp, Belgium, info@maklu.be
Koninginnelaan 96, 7315 EB Apeldoorn, The Netherlands, info@maklu.nl
www.maklu.eu

USA & Canada
International Specialized Book Services
920 NE 58th Ave., Suite 300, Portland, OR 97213-3786, orders@isbs.com,
www.isbs.com

Surveillance for public security purposes

Four pillars of acceptable interference with the fundamental right to privacy

WOJCIECH R. WIEWIÓROWSKI[1]

1. INTRODUCTION

The problem of global surveillance systems introduced by the governments of world superpowers became one of the main leitmotifs of privacy disputes, if not the leading one, after Edward Snowden's revelations in 2013. The idea of a universal panopticon[2] was confronted with the lawful interception[3] into the private life of individuals which is introduced in order to protect society. Such intrusion had been justified already for a decade when Snowden became a prophet of the new era of state surveillance[4] with a vision of the American National Security Agency (NSA) being a modern incarnation of Foucault's panopticon[5] – a concept that was one of the main architectural structures of

[1] European Data Protection Assistant Supervisor (since December 2014); Adjunct professor, University of Gdansk, Division of Legal Informatics; Inspector General for the Protection of Personal Data (GIODO) (2010-2014); Vice Chairman, Working Party Art. 29 (February-November 2014). Email: wojciech.wiewiorowski@edps.europa.eu.

[2] David Friedman, *Future Imperfect: Technology and Freedom in an Uncertain World* (Cambridge University Press 2008) 66-79.

[3] Doctrine often exchange notions of "lawful interception" and "surveillance" stating that the lawful interception of meta-data is a targeted surveillance required by law enforcement authorities and should not be considered as mass surveillance. See: Stefan Schuster (ed.), *Mass Surveillance: Part 1 - Risks and opportunities raised by the current generation of network services and applications* (STOA Report European Parliamentary Research Service, Brussels, 2015) 8.

[4] Daniel Knapp, 'The Social Construction of Computational Surveillance: Reclaiming Agency in a Computed World' (PhD thesis, London School of Economics and Political Science 2016) 26.

[5] Sarah Horowitz, 'Foucault's Panopticon: A Model of NSA Surveillance?' in Russel A. Miller, *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair*, (CUP 2017) 39-62. See also: Sergei Boeke and Quirine Eijkman, 'State Surveillance in Cyber Space: A new perspective on digital data practices by intelligence dervices' in Lee Jarvis, Stuart MacDonald, Thomas M. Chen (ed.), *Terrorism Online: Politics, Law and Technology* (Routledge 2016) 128-131 and Richard Stiennon, *There Will Be*

the surveillance discussion, both in Europe and at a global level.[6] Although surveillance should not always be treated as an obstruction to privacy and vice versa[7], most commentaries link the current discussion to Orwell's or Kafka's dystopias[8].

2. EUROPEAN ESSENTIAL GUARANTEES

In the heart of the discussion on the new solution, which was expected to replace the *Safe Harbour Agreement*, the Article 29 Working Party[9] – representing all European data protection authorities (DPAs) – formulated a list of requirements for surveillance mechanisms that interfere with the right to privacy and data protection. Later judgments of the Court of Justice of the European Union have confirmed the line of reasoning used by the DPAs, and four relevant pillars of accepted activity at the time of rising insecurity – known as '*European Essential Guarantees*' – have been described. They consist of:

a. the requirement that the processing should be based on clear, precise and accessible rules;

b. demonstration of the necessity and proportionality with regard to the legitimate objectives pursued;

c. existence of an independent oversight mechanism as well as

Cyberwar: How The Move To Network-Centric War Fighting Has Set The Stage For Cyberwar (IT-Harvest Press 2015) 67-77 on NSA offensive cyber capabilities.

[6] Knapp (n 4) 32-36.

[7] On unusual alliances between privacy and surveillance see Gary T. Marx, 'Coming to Terms: The Kaleidoscope of Privacy and Surveillance' in Beate Roessler and Dorota Mokrosinska (ed.) *Social Dimensions of Privacy: Interdisciplinary Perspectives* (CUP 2015) 33-34.

[8] Recapitulation of both aspects of surveillance almost ten years before Snowden's revelations: Daniel Solove, *The Digital Person: Technology and privacy in the information age* (NYU Press 2004) 168-180.

[9] Working Party on the Protection of Individuals with regard to the Processing of Personal Data established on a basis of Article 29 of the Directive 95/46/EC. It is an independent European advisory body on data and privacy protection, composed of data protection commissioners of all European Union Member States. The tasks of the group are specified in Article 30 of the Directive 95/46/EC and Article 15 of the Directive 2002/58/EC.

d. availability of effective remedies to the individual.[10]

The right to the protection of personal data as well as the right to respect for private life are included in the Charter of Fundamental Rights, and were later also enshrined in the Treaty on the Functioning of the European Union. Neither of them is an absolute right and there is no doubt they may be limited, provided that the limitations comply with the requirements laid down in Article 52(1) of the Charter itself. The limitation has to be lawful, meaning it should be provided for by law and should respect the essence of the rights. It must also genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. Moreover, the principles of necessity and proportionality of such limitations have to be observed.

3. PROVIDED BY LAW

The Article 29 Working Party started its deliberation by explaining the first fundamental principle - i.e. the processing should be based on clear, precise and accessible rules - with reference to the foreseeability of the interference even when the action is justified. Using jurisprudence of the European Court of Human Rights (ECtHR), the Working Party states that it should be possible to assess the effect of the interference on the individual, in order to give the person an adequate protection against arbitrary actions of the state. In its judgment on the *Malone* case, the Strasbourg Court stressed that the processing must be based on a precise, clear and accessible legal basis[11]. Such a legal basis should be set out in statute law which is easily accessible for the public and which should explain the nature of the offences that may give rise to an interception or surveillance order. The law should also define the categories of people that might be subject to surveillance. The measures taken should be limited as far as the duration is concerned. Last but not least, recalling the judgment in *Weber and Saravia*, DPAs reaffirm that the procedure to be followed for examining, using and storing the data obtained, the precautions to be taken when communicating the data to other parties and the circumstances in which the materials that result from such an interference may

[10] Article 29 Working Party, Working Document 1/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) (WP 237) 7 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf>.

[11] *Malone v the United Kingdom* App no 8691/79 (ECtHR, 2 August 1984) para 67.

or must be destroyed, have to be foreseeable as well[12]. It is clear that the risks of arbitrariness are especially evident where a power vested in the executive is exercised in secret[13]. The law must include sufficiently clear terms in order to give citizens an adequate indication as to the circumstances in which and the conditions according to which public authorities are empowered to resort to such measures.

The same principle was recalled by the Strasbourg Court in its most important recent case *Zakharov v Russia*[14], which supplemented its line of interpretation and explained that the reference to "foreseeability" in the context of interception of communications cannot be the same as in many other fields. Foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. The law in Member States that are parties to the Convention must be sufficiently clear in order to give citizens an adequate indication as to when and how public authorities may resort to surveillance measures.

---

[12] *Weber and Saravia* v *Germany* App no 54934/00 (ECtHR, 29 June 2006) para 95. See also: *Huvig* v *France* App no 11105/84 (ECtHR, 24 April 1990) para 34; *Kopp v Switzerland* App no 23224/94 (ECtHR, 25 March 1998) para 55; *Amann v Switzerland* App no 27798/95 (ECtHR, 16 February 2000) para 76; *Valenzuela Contreras v Spain* App no 27671/95 (ECHR, 30 July 1998) para 46; *Prado Bugallo v Spain* App no 58496/00 (ECtHR, 18 February 2003) para 30. More on that in Lee Andrew Bygrave, *Data Privacy Law. An International Perspective* (OUP 2014) 93-94.

[13] *Rotaru v Romania* App no 28341/95 (ECtHR, 4 May 2000) para 55; *Huvig v France* App no 11105/84 (ECtHR, 24 April 1990) para 29; *Zakharov v Russia* App no 47143/06 (ECHR, 4 December 2015) para 229. See also: Susana Sanchez Ferro, 'The Need for an Institutionalized and Transparent Set of Domestic Legal Rules Governing Transnational Intelligence Sharing in Democratic Societies' in Miller (n 5) 513.

[14] *Zakharov* (n 13). One of the leading ECHR judgements concerned the system of secret interception of mobile telephone communications in the Russian Federation. The applicant – an editor-in-chief of a publishing company – complained that Russian law permitted blanket interception of communications by law enforcement agencies. The Court held that there had been a violation of Article 8 of the Convention, finding that the Russian legal provisions governing interception of communications did not provide for adequate and effective guarantees against arbitrariness and the risk of abuse which was inherent in any system of secret surveillance, and which was particularly high in a system such as in Russia where the secret services and the police had direct access, by technical means, to all mobile telephone communications. Moreover, the effectiveness of the remedies available to challenge interception of communications was undermined by the fact that they were available only to persons who were able to submit proof of interception.

The Strasbourg Court ruled similarly four years ago in another Russian case initiated by *Sergiey M. Shimovolos*[15]. This case concerned the registration of a human rights activist in the so-called "surveillance database", which collected information about his movements, by train or air, within Russia, and about his arrest. The Court held that there had been a violation of Article 8 of the Convention. The judges observed that the creation and maintenance of the database and the procedure for its operation were governed by a ministerial order which had never been published or otherwise made accessible to the public. Consequently, the Court found that the domestic law did not indicate with sufficient clarity the scope and manner of exercising the discretion conferred on the domestic authorities to collect and store information on individuals' private lives in the database. In particular, it did not set out any indication of the minimum safeguards against abuse in a form accessible to the public.

4. NECESSITY AND PROPORTIONALITY

Hustinx is surely right when he writes that the European Human Rights Convention's approach is not that processing of personal data should always be considered as an interference with the right to privacy, but rather that for the protection of privacy and other fundamental rights and freedoms, any processing of personal data must always observe certain legal conditions. Such a legal condition could be the principle that personal data may only be processed for specified legitimate purposes, where necessary for these purposes, and not used in a way incompatible with those purposes. Under this approach, the core elements of Article 8 ECHR, such as that the right to privacy may only be interfered with when there is an adequate legal basis and a legitimate purpose, have been transferred into a broader context. This only works well in practice if the system of checks and balances, as set out in the Convention - consisting of substantive conditions, individual rights, procedural provisions and independent supervision - is sufficiently flexible to take account of variable contexts, and is applied with pragmatism and an 'open eye' for the interests of data subjects and other relevant stakeholders[16].

Nevertheless, all kinds of processing of personal data by government authorities are often regarded as an interference with the right to privacy and data

---

[15] In *Shimovolos v Russia* App no 30194/09 (ECtHR, 21 June 2011) the Court also held that there had been a violation of Article 5 (right to liberty and security) of the Convention.

[16] Peter Hustinx, 'European Leadership in Privacy and Data Protection' in Artemi Rallo Lombarte and Rosario García Mahamut (eds) *Hacia un nuevo régimen europeo de protección de datos* (Tirant Lo Blanch 2015) 18.

protection as they are described in the Charter and the Treaty. As it was stated before, such an action by the government – including data processing for intelligence purposes – can be justifiable only when it is necessary and proportionate in relation to a legitimate objective[17]. The Court of Justice of the EU has made it clear in its judgement in *Schrems*, that the "legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data (…) without any differentiation, limitation or exception being made in the 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"[18].

The same line of interpretation was also taken by the European Court of Human Rights in its leading judgement on state surveillance last year – *Szabó and Vissy v Hungary*[19] – when the ECHR stated that "in the face of this progress the Court must scrutinise the question as to whether the development of surveillance methods resulting in masses of data collected has been accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights. (…) Indeed, it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives. (…) This threat to privacy must be subjected to very close scrutiny both on the domestic level and under the Convention. (…) However, it is not warranted to embark on this matter in the present case". The Court accepted that it was a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies, including massive monitoring of communications, in pre-empting impending incidents. However, the Court was not convinced that the legislation in question provided sufficient safeguards to avoid abuse. The scope of the measures could virtually include anyone in Hungary, and with

[17] Bygrave (n 12) 94-96 and 147-150.

[18] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* EU:C:2015: 650, para 95.

[19] *Szabó and Vissy v Hungary* App no. 37138/14 (ECtHR, 12 January 2016) paras 68-70. The Court further held that there had been no violation of Article 13 (right to an effective remedy) of the Convention taken together with Article 8, reiterating that Article 13 could not be interpreted as requiring a remedy against the state of domestic law.

new technologies the Government could easily intercept masses of data concerning even persons outside the original range of operation. Furthermore, according to the Court, the ordering of such measures was taking place entirely within the realm of the executive, without an assessment of whether interception of communications was strictly necessary and without any effective remedial measures, let alone judicial ones, being in place.

The Luxembourg Court has joined this line of interpretation in the *Digital Rights Ireland* case[20], invalidating the so-called Data Retention Directive[21]. The Court assessed the European Union legislation and found that it covers "all persons and all means of electronic communication" without "any differentiation, limitation or exception being made". Thus, the Court considered that the legislator failed to provide for an "objective criterion by which to determine the limits of the access (…) and their subsequent use".[22]

It was already after the Article 29 Working Party passed its working document on the essential guarantees that the Court of Justice confirmed these lines of reasoning in two judgments connected with the legality of the massive and indiscriminate collection of personal data and their re-use.

In the judgment on the joined cases *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson and Others* [23] – revealed just before Christmas 2016 and thus summarising the year spent on discussing on the guarantees – the Court of Justice reaffirmed the *Digital Rights Ireland* decision on the retention of telecommunication data and assessed the Swedish and UK domestic regime. It made clear that the data retention laws of Member States must comply with EU data protection rules even in absence of the special legal act of the secondary law devoted to that

[20] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* EU:C:2014:238.

[21] Parliament and Council Directive 2006/24/EC of 15 March 2006 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 2002/58/EC [2006] OJ L105/54.

[22] For an in-depth analysis of the access to private resources by state authorities (incluing data on France, Germany, Israel, Italy, Brasil, Canada, US, Australia, China, India, Japan and Korea), see Fred H Cate, James X Dempsey (eds), *Bulk Collection: Systematic Government Access to Private-Sector Data* (Oxford University Press 2017).

[23] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Davis and Others* EU:C:2016:970.

matter, and that generalised and indiscriminate surveillance is not permissible under EU law. The Court admitted that "a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offenses, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security", and thus data retention itself might be lawful if limited. The criteria which a national data retention law needs to contain include clear and precise rules and impose minimum safeguards set in the law, as well as indications of circumstances and conditions under which data retention may be adopted as a preventative measure.

The Court failed to find a significant difference between the notions of "retention" and "processing of data" stating that the latter, in connection with provisions on electronic communications, also covers the intermediate retention of such data of the relevant communications. The Court's judgement in *Tele2 Sverige* is mainly based on a proportionality assessment weighing the right to data protection versus the demands of public security concerns.

Further legal analysis on the necessity, including the necessity test applied to the right to the protection of personal data, has been provided by the European Data Protection Supervisor in 2017 in the toolkit published to help EU institutions to interpret particular requirements stemming from Article 52(1) of the Charter, in which it is stated that any limitation on the exercise of the right to personal data protection (Article 8 of the Charter) must be "necessary" for an objective of general interest or to protect the rights and freedoms of others[24].

The EDPS finds that the next test should assess whether the measure meets an objective of general interest. The objective of general interest provides the background against which the necessity of the measure may be assessed. It is therefore important to identify the objective of general interest in sufficient detail in order to allow the assessment as to whether a proposed measure, which entails the processing of personal data, is really necessary. If this test is satisfied, the proportionality of the envisaged measure will be assessed. Should the draft measure not pass the necessity test, there is no need to examine its proportionality. A measure that has not proved to be necessary should not be proposed unless and until it has been modified to meet the requirement of necessity. A proper description of the measure is, in the Supervisor's view, important as it may affect several of the criteria mentioned earlier by the Courts. The Courts, therefore, may sometimes assess the criteria in

[24] European Data Protection Supervisor (EDPS), Assessing the necessity of measures that limit the fundamental right to the protection of personal data (a toolkit), <https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf >.

tandem. For instance, a measure that is unclearly or too broadly defined may prevent an assessment of whether it is "provided by law" and "necessary".

The EDPS also studies the relationship between proportionality and necessity, reminding that proportionality is a general principle of EU law which requires that "the content and form of Union action shall not exceed what is necessary to achieve the objectives of the treaties". He quotes the *Gauweiler* judgment stressing that "the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives"[25]. It therefore, recalling judge Lenaerts, "restricts the authorities in the exercise of their powers by requiring a balance to be struck between the means used and the intended aim (or result reached)"[26].

Proportionality in a broad sense encompasses both the necessity and the appropriateness of a measure; namely the extent to which there is a logical link between the measure and the (legitimate) objective pursued. Furthermore, for a measure to meet the principle of proportionality as enshrined in Article 52(1) of the Charter, the advantages resulting from the measure should not be outweighed by the disadvantages the measure causes with respect to the exercise of the fundamental rights. This latter element describes proportionality in a narrow sense and consitutes the proportionality test. It should be clearly distinguished from necessity. Necessity implies the need for a combined, fact-based assessment of the effectiveness of the measure for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal[27].

Finally, the EDPS states that "necessity" is also a data quality principle and a recurrent condition in almost all the requirements on the lawfulness of the processing of personal data stemming from EU data protection secondary law. There is also a link between Article 8(2) of the Charter and the secondary law, as Article 8(2) refers to the legitimate basis for processing "laid down by

---

[25] Case C-62/14 *Peter Gauweiler and Others v Deutscher Bundestag* ECLI:EU:C:2015: 400, [2015], para 67, on request for a preliminary ruling from the Bundesverfassungsgericht. The case concerned the legality of the decision of the Governing Board of the European Central Bank of September 2012 on so called 'Outright Monetary Transactions' (OMT).

[26] Koen Lenaerts and Piet Van Nuffel, *European Union Law* (3rd edn, Sweet & Maxwell 2011) 141.

[27] ibid 24, 5.

law" and the Explanatory Note on Article 8 refers to this secondary law stating that the Directive 95/46 and the Regulation 45/2001 "contain conditions and limitations for the exercise of the right to the protection of personal data".

The question of whether a measure should target any crime or only serious crimes may be considered a matter of necessity; however, should such a provision be assessed to be necessary, an assessment of its proportionality and its risk of eroding the values of a democratic society would still be needed. Therefore, in practice, there is some overlap between the notions of necessity and proportionality, and, depending on the measure in question, the two tests may be carried out concurrently or even in a reverse order. In *Digital Rights Ireland*, the Court first stated that proportionality consists of the steps of appropriateness and necessity[28]. It then established that the limitation of the rights protected in Articles 7 and 8 were not necessary[29] and therefore concluded, that the limitations were not proportionate[30]. Also in *Schrems*[31] the Court analysed the necessity and found the Safe Harbour Decision to be invalid without making any reference to proportionality before reaching this conclusion. The Court of Justice is clear when it comes to the content of communications data and states in *Schrems* that public authorities should not be allowed to have access to the content of electronic communications on a generalised basis.[32] It should be also noted that the Article 29 Working Party underlined that an interference takes place not only at the time of collection of the data, but also everytime the data is accessed by a government authority for further processing for intelligence purposes[33].

---

[28] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* EU:C:2014:238, para 46. On more general consequences of this judgement: Sergio Carrera and others, *Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights* (CEPS 2015) 74.

[29] ibid, para 65.

[30] ibid, para 69.

[31] *Maximillian Schrems* (n 18) paras 92-93 and 98.

[32] On the dichotomy between law enforcement and intelligence: Liane Colonna, *Legal Implications of Data Mining: Assessing the European Union's Data Protection Principles in Light of the United States Government's National Intelligence Data Mining Practices* (PhD thesis, Stockholm University 2016) s 193. See also: *Fundamental Rights Agency, Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II: field perspectives and legal update* (Fundamental Rights Agency 2017) 28.

[33] *Maximillian Schrems* (n 18) para 95; *Uzun v Germany* App no 35623/05 (ECtHR, 2 September 2010), para 63; Hielke Hijmans, *The European Union as a Constitutional*

5. AN INDEPENDENT OVERSIGHT MECHANISM

Another pillar which is absolutely necessary in order to recognise that an interference with the right to privacy and data protection is acceptable, according to the Article 29 Working Party, is the existence of an effective, independent and impartial oversight system, in the form of either a judicial review or an activity of another independent body, such as an administrative authority or a parliamentary committee[34]. Regardless of the form of the independent supervision[35], the existence of oversight authorities forms "an essential component of the protection of individuals with regard to the processing of personal data"[36].

Hijmans deliberates on the reasons for having an independent authority in place and recapitulates a number of them as essentially convincing that an independent oversight system is necessary[37]. The oversight should be carried out by a public body (1) which acts effectively (2). The body, or rather its representatives, should know the nature of data processing and be skilled to assess it (3) and their approach to the duties of controllers should be consistent to different sectors, private or public (4). The body has to be independent from political influences (5) and, in Hijman's view, an advantage is given to institutions established solely for privacy and data protection.

The independent oversight can take place at various stages during the lifecycle of a data processing operation. It can start when the surveillance is first ordered, but it can also begin while it is being carried out and even after it has been terminated. Depending of the nature of the activities and on some external circumstances, either a prior or ex-post analysis can be recognised as acceptable according to the standards[38]. In *Zakharov,* the ECtHR has accepted the fact that the special nature of data processing for intelligence purposes makes it acceptable that the processing itself takes place without the data subject being informed. The judges write that "as regards the first two stages,

Guardian of Internet Privacy and Data Protection: The Story of Article 16 TFEU (Springer 2016) 267.

[34] *Klass and Others v Germany* App no 5029/71 (ECtHR, 6 September 1978) paras 17 and 51.

[35] See analysis in Hijmans (n 33) 385-391.

[36] Case C-518/07 *European Commission v Germany* ECLI:EU:C:2010:125, [2010] ECR I-01885, para 23.

[37] Hijmans (n 33) 352-355.

[38] *Klass* (n 34) paras 55-56; *Zakharov* (n 13) para 233.

the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be affected without the individual's knowledge. (…) In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure."[39]

A similar line is taken by the CJEU in *Digital Rights Ireland* where the Court states that "the access (…) to the data retained [should also be] made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions."[40] The Court made these matters clear by holding that the Data Retention Directive was invalid because it did not meet these requirements[41].

Both the Strasbourg and Luxembourg Court studied the status of the oversight organ. The ECtHR prefers the independence of oversight mechanisms, including the judge, yet exceptions are acceptable "as long as [the supervisor] is sufficiently independent from the executive."[42] The CJEU accepts that the oversight is given to administrative bodies in the European Union. Their status was especially examined in three cases on the independence of the data protection authorities in Germany[43], Austria[44] and Hungary[45].

[39] *Zakharov* (n 13) para 233.

[40] *Digital Rights Ireland* (n 20) para 62.

[41] Hijmans (n 33) 268-272.

[42] *Zakharov* (n 13) para 258.

[43] Case C-518/07 *European Commission v Germany* ECLI:EU:C:2010:125, [2010] ECR I-01885.

[44] Case C-614/10 *Commission v Austria* ECLI:EU:C:2012:631, [2012].

[45] Case C-288/12 *Commission v Hungary* ECLI:EU:C:2014:237, [2014].

6. EFFECTIVE REMEDIES AVAILABLE TO THE INDIVIDUAL

The final European Essential Guarantee is related to the effective[46] redress rights of the individual. The CJEU explained in *Schrems* that the essence of the right to an effective remedy was affected. It was stated that "[l]egislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter"[47] . Therefore, the Court did not even start the examination of whether such a limitation was necessary and instead decided to invalidate the whole Commission Decision on the adequacy of the Safe Harbour Principles[48].

The strongest comment on this point was provided by the German Schleswig-Holstein data protection authority, who stated in the position paper on the judgment: "If citizens of the European Union have no effective right to access their personal data or to be heard on the question of surveillance and interception and to enjoy legal protection, article 47 of the CFR is infringed (...) The USA can currently show no effective means to ensure protection essentially equivalent to the level of protection guaranteed within the European Union"[49].

---

[46] On effectiveness Hijmans (n 33) 382.

[47] *Maximillian Schrems* (n 18) para 95.

[48] Martin A. Weiss and Kristin Archick, 'U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield, Congressional Research Service report' <https://fas.org/sgp/crs/misc/R44257.pdf>. For the analysis of later developments and their critical review see: Peter Swire, 'US Surveillance Law in a constitutional democracy, Safe Harbor, and Reforms since 2013' (Georgia Tech Scheller College of Business Research Paper no 36); Gert Vermeulen, 'The Paper Shield. On the degree of protection of the EU-US Privacy Shield against unnecessary or disproportionate data collection by the US intelligence and law enforcement services' in Dan Svantesson and Dariusz Kloza, *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy* (Intersentia 2017) 85-126 and 127-147. See also: David Vladeck, 'Separated by Common Goals: A U.S. Perspective on Narrowing the U.S.-E.U. Privacy Divide' in Rallo Lombarte and Mahamut (eds) (n 16) 207-243.

[49] *ULD position paper on the judgment of the Court of Justice of the European Union of 6 October 2015, C-362/14* <https://www.datenschutzzentrum.de/uploads/internationales/20151014_ULD-PositionPapier-on-CJEU_EN.pdf>. See also: Shara Monteleone and Laura Puccio, *From Safe Harbour to Privacy Shield: Advances and shortcomings of the new EU-US data transfer rules* (In-Depth Analysis, European Parliamentary Research Service 2017) 11 <http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/595892/EPRS_IDA(2017)595892_EN.pdf >.

For the Strasbourg Court, the question of an effective remedy[50] is inextricably linked to the notification of the individual with regard to a surveillance measure once the surveillance is over. The Article 29 Working Party rightly cites the *Zakharov* case, where the ECtHR stated that "there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively or, in the alternative, unless any person who suspects that his or her communications are being or have been intercepted can apply to courts, so that the courts' jurisdiction does not depend on notification to the interception subject that there has been an interception of his communications".[51]

Where no notification has been given, the ECtHR established criteria that have to be met by the independent authority. It has to be an independent and impartial body, which has adopted its own rules of procedure, and which consists of members that must hold or have held high judicial office or must be experienced lawyers. The body should be able to access all relevant information when it examines complaints by individuals, including all kinds of confidential materials[52]. Examining the case of *Uzun v Germany*[53], the Court held that there had been no violation of Article 8 of the Convention. Given that the criminal investigation had concerned serious crimes, it found that the GPS surveillance of the applicant had been proportionate, while the applicant, suspected of involvement in left-wing terrorist extremism, complained that surveillance by GPS and the use of collected data in the criminal proceedings against him had violated his right to respect for private life[54].

---

[50] On the possible role of class action Marc Rotenberg and others, 'Enforcing Privacy Rights: Class Action Litigation and the Challenge of cy pres' in David Wright and Paul de Hert (eds), *Enforcing Privacy. Regulatory, Legal and Technical Approaches* (Springer 2016) 307-334.

[51] *Zakharov* (n 13) para 234.

[52] *Kennedy v The United Kingdom* App no 26839/05 (ECtHR, 18 May 2010) para 167. However, it is not easy to reach this purpose as the long list of national case law shows in Didier Bigo and others, 'National Security and Secret Evidence in Legislation and before the Courts: Exploring the Challenges' (CEPS 2014) 77-79 <http://www.europarl.europa.eu/RegData/etudes/STUD/2014/509991/IPOL_STU(2014)509991_EN.pdf>.

[53] *Uzun v Germany* App no 35623/05 (ECtHR, 2 September 2010).

[54] A similar case – *Ben Faiza v France*, App no 31446/12 (ECtHR) – is still pending in the Court, being communicated to the French Government on 3 February 2015. The complainant protests against an interference with his private life on account of the

7. THE COURT OF JUSTICE CONFIRMS THE EUROPEAN ESSENTIAL GUARANTEES

The *Digital Rights Ireland* case had an enormous impact across the EU, but particularly in the United Kingdom close attention was being paid to the judgment.[55] The immediate effect of the judgment was however far from the expectations of privacy advocates, since some of the EU Member States logically understood that the invalidation of the Data Retention Directive actually gives the states much more flexibility. So far, the sector was co-regulated, but when the EU component of the co-regulation vanished, the only remaining part falls within the discretion of the state in light of the subsidiarity principle. This, however, was challenged by privacy advocates who still saw Article 15 of the ePrivacy Directive as the basis for co-regulation.

Subsequent activities of the Swedish[56] and UK governments led to the next important case in Luxembourg, which was expected to filter the *Digital Rights Ireland* judgement test in the joined cases *Tele2 and Watson (ex-Davis)*[57]. The first concerned the Swedish Tele2 company which decided to cease retaining data. The second involved the '*Data Retention and Investigatory Powers Act' (DRIPA)*, which was adopted by the UK government in 2014, and later challenged by British parliamentarians. The cases had first been assessed by Advocate General *Saugmandsgaard Øe* on 19 June 2016 and were finally judged by CJUE half a year later[58]. The Advocate General had no doubts that Article 51 of the Charter of Fundamental Rights is fully applicable to national provisions implementing Article 15 of the ePrivacy Directive. At the same time, he admitted that a general retention of communications may be compatible with the EU law subject to satisfying strict requirements set out by the ePrivacy Directive and the Charter. The Court followed this line of interpretation and underlined that derogations are acceptable only insofar as strictly necessary.

---

installation of a GPS tracking device in his vehicle with the aim of monitoring his movements during the course of a drug trafficking inquiry.

[55] Lucia Zedner, 'Why Blanket Surveillance Is No Security Blanket: Data Retention in the United Kingdom after the European Data Protection Directive' in Miller (n 5) 564-585.

[56] See also another case against Sweden still pending before the ECtHR: *Centrum För Rättvisa v Sweden*, App no 35252/08. The application was communicated to the Swedish Government on 21 November 2011 and 14 October 2014. The applicant, a non-profit public interest law firm, complains about the Swedish state practice and legislation concerning secret surveillance measures.

[57] *Tele2 Sverige AB* (n 22).

[58] On 21 December 2016.

Applying these rules to the facts of cases, the CJUE held that the retention of metadata is as revealing as the retention of the content since it makes profiling possible[59] and, furthermore,the data in question is liable to allow very precise conclusions to be drawn on private lives. The social knowledge on the retention gives people the feeling that they are under constant surveillance. It then affects the use of communications and the right to freedom of expression. In consequence, the Court accepted such actions only in case of serious crimes, stating that such a justified interference cannot be implemented into national legislation by provisions on the general and indiscriminate retention of data.[60]

The proportionality of intrusion has been also studied extensively when the Court of Justice was asked by the European Parliament for an opinion on the EU-Canada agreement on exchange of Passenger Name Records (PNR)[61]. Once again, the European Court confirmed that the European Commission failed to understand which legal requirements are to be observed when the,

---

[59] The distinction of communication metadata and content metadata was omitted since from a legal perspective, the communication meta-data is the only existing metadata, as content meta-data is considered to be part of the content and travels end-to-end embedded in the content. The structured nature of the meta-data is ideally suited for analysis using data mining techniques such as pattern recognition, machine learning, and information or data fusion. See: Schuster (n 3) 7 and 9.

[60] Other pending Strasbourg cases to be observed in this matter are: a) *Tretter and Others v Austria* (App no 3599/10 communicated to the Austrian Government on 6 May 2013) on amendments of the Police Powers Act extending the powers of the police authorities to collect and process personal data; b) *Big Brother Watch and Others v the United Kingdom* (App no 58170/13 communicated to the UK Government on 9 January 2014) on three NGOs and one academic working internationally likely being subjects of surveillance by UK intelligence services; c) *Bureau of Investigative Journalism and Alice Ross v the United Kingdom* (App no 62322/14 communicated to the UK Government on 5 January 2015) interception of both internet and telephone communications by government agencies and blanket interception, storage and exploitation of communication amount to disproportionate interference with journalistic freedom of expression and d) *Association confraternelle de la presse judiciaire v France et 11 autres requêtes* (App nos 49526/15, 49615/15, 49616/15, 49617/15, 49618/15, 49619/15, 49620/15, 49621/15, 55058/15, 55061/15, 59602/15 and 59621/15 communicated to the French Government on 26 April 2017) lawyers and journalists and legal persons connected with these professions, concern the French Intelligence Act of 24 July 2015.

[61] Earlier history of PNR agreements negotiated by EU is summarised in Mistale Taylor, 'Flying from the EU to the US: necessary extraterritorial legal diffusion in the US-EU Passenger Name Record agreement' (2015) 19 Spanish Yearbook of International Law 223-225.

generally acceptable, idea of PNR finds its implementation into statutory law.[62] On 26 July 2017, the Court declared that the agreement may not be concluded in the form passed to the European legislator[63]. The Parliament referred the agreement to the Court in order for the regularity of the agreement to be assessed under EU law, and in particular the Charter of Fundamental Rights of the European Union. In its Opinion, the CJEU declared that this retention of bulk data is excessive and would therefore violate fundamental rights of EU citizens. The Court of Justice admitted that the transfer itself, even when made on a systematic basis, the retention and the use of all PNR are, in essence, permissible; yet the Court agreed with the Parliament that several provisions of the draft agreement did not meet the requirements stemming from the fundamental rights of the European Union[64]. The Court questioned the systematic and continuous transfer of data of all air passengers to a Canadian authority with a view to that data being used and retained and possibly subsequently transferred to other authorities and other non-member countries, for the purpose of combating terrorism and serious transnational crime. Since the period during which the PNR data may be retained may last for up to five years, this agreement makes it possible for information on the private lives of passengers to be available for a particularly long period of time.

The Court stated that the EU-Canada agreement should determine in a more clear and precise manner how PNR data may be transferred. It should also require that the models and criteria used for the automated processing of the PNR data are specific, reliable and non-discriminatory. The use of databases should be only limited to the fight against terrorism and serious transnational crime. The law should also provide for a right to individual notification for air passengers in the event of use of the PNR data concerning them during their stay in Canada and after their departure from that country, as well as in the event of disclosure of that data to other authorities or to individuals. The Court required the guarantee that the oversight of the rules relating to the protection of air passengers with regard the processing of the PNR data is

---

[62] European Digital Rights (EDRi), 'European Court Opinion: Canada PNR cannot be signed' (2016), <https://edri.org/european-court- opinion-canada-pnr-deal-cannot-be-signed/>.

[63] Hielke Hijmans, 'PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators' (2017) European Data Protection Law Review 310-312.

[64] Short description of EU PNR schemes in Wim Wensink and others, *The European Union's Policies on Counter-Terrorism: Relevance, Coherence and Effectiveness* (Study for the LIBE Committee 2017) 121-123 <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/ 583124/IPOL_STU(2017)583124_EN.pdf>.

carried out by an independent supervisory authority[65]. Finally, it observed that the interferences which the envisaged agreement entails were not all limited to what is strictly necessary and were therefore not entirely justified[66].

The previous opinion in this case, issued by Advocate General Mengozzi on 8 September 2016, stressed that the draft agreement was not ready to be ratified, because it was incompatible with Article 16 TFEU and Articles 7 and 8 of the Charter. Expressing the need for a fair balance between public security and privacy and data protection, Mengozzi established lists of compatibility requirements and incompatibility features in relation to the Charter. The list of requirements for compatibility included: clear categories of attributes of PNR (with no sensitive data included), an exhaustive list of offences, identification of an authority responsible for PNR oversight, limitation of targets to reasonable suspicion, limited and specified access rights and justification for a five-year-retention period. Mengozzi also required a prior review of transfers and the monitoring by an independent Canadian authority. At the same time, his list of incompatibilities with the Charter referred to: the processing of PNR data outside the public security objective of fighting terrorism and serious transnational crime, processing of sensitive data, the right to disclose information beyond the objective, authorisation to retain PNR data for five years beyond the objective as well as transfers without prior assessment by the competent Canadian authority.

In its judgment, the Court held that all international agreements form part of the EU legal order and must be compatible with the Treaties and principles and that the PNR agreement between EU and Canada is an external equivalent of a legislative act. In the view of the Court, processing of PNR, as it is with all personal data, affects the right to privacy and data protection. It can be justified that the legitimate objectives of protecting public security, fighting terrorism and serious transnational crime are good excuses if the agreement does not adversely affect the essence of either right.

Nevertheless, the necessity of such intrusion was not clear and the agreement neither sufficiently specified the personal data to be transferred nor did it justify the processing of sensitive data for the purposes revealed. Machine models and criteria used to analyse PNR must be specific, reliable and non-

---

[65] See also Opinion C-1/15 *European Commission v Republic of Austria*, ECLI:EU:C:2016:656, Opinion of AG Mengozzi <http://curia.europa.eu/juris/documents.jsf?num=C-1/15>.

[66] *EU and Canada PNR Agreement Invalid* (SCL The IT Law Society 2016), <https://www.scl.org/news/3734-eu-and-canada-pnr-agreement-invalid>.

discriminatory, while cross-checking databases must be accurate and appropriate. The primary purpose of such processing should be, in the opinion of the Court, limited to what is strictly necessary. The retention of the data of all passengers after their departure from Canada is not strictly necessary, while it may be justifiable to retain data on specific individuals if based on objective criteria and following a prior review of the court or an independent body. The Court of Justice stated that the agreement did not guarantee in a sufficiently clear and precise manner the oversight of data protection safeguards by an independent authority not subject to external influence. In conclusion, the current draft of the agreement was incompatible with Articles 7, 8, 21 (non-discrimination) and 52(1) of the Charter.

8. EPILOGUE

The current discussion on the European expectations towards guarantees given for transfer of data outside the zone recognised as secure and on the future of domestic data protection regimes in what was a third pillar of the European Union in the past, takes place at the same time as two other challenges. American lawmakers are working on the reform of FISA Section 702, remembering it will expire on 31 December 2017. The so-called "Section 702" is still the main legal basis for mass surveillance activities in the United States, including the programs and tools used in case of data stored by non-US persons and entities on American servers[67].

At the same time, the actions by Maximilian Schrems continue and are expected to reach the Court of Justice in Luxembourg again. In the next months, another look will be taken at how US law protects the privacy rights of European customers, possibly together with the Court's assessment of the new Privacy Shield agreement. Both factors may significantly affect the practice of international transfers of data. Nevertheless, the principles described by the Article 29 Working Party and confirmed by the Courts in Luxembourg and Strasbourg will definitely stay the same.

9. SELECTED LITERATURE

Bignami F, *The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens* (Study for the LIBE

[67] Fransesca Bignami, *The US Legal System on Data Protection in the Field of Law Enforcement. Safe-guards, Rights and Remedies for EU Citizens* (Study for the LIBE Committee 2015) 22-29 <http:// www.europarl.europa.eu/RegData/etudes/STUD/2015 /519215/IPOL_STU(2015) 519215_EN.pdf>.

Committee 2015) <http://www.europarl.europa.eu/RegData/etudes/STUD /2015/519215/ IPOL_STU(2015)519215_EN.pdf>

Bigo D and others, 'National Security and Secret Evidence in Legislation and before the Courts: Exploring the Challenges' (2015) 78 Liberty and Security in Europe 77-79 <http://www. europarl.europa.eu/RegData/etudes/STUD/ 2014/509991/IPOL_STU (2014)509991_EN.pd.>

Boeke S and Eijkman Q, 'State Surveillance in Cyber Space: A new perspective on digital data practices by intelligence dervices', in Jarvis L, MacDonald S and Chen T M (ed.) *Terrorism Online: Politics, Law and Technology* (Routledge 2016) 128-131

Bygrave L A, *Data Privacy Law. An International Perspective* (Oxford University Press 2014)

Carrera S and others, *Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights* (Centre for European Policy Studies Study 2015) 74

Cate F H, Dempsey J X (eds) *Bulk Collection: Systematic Government Access to Private-Sector Data* (Oxford University Press 2017)

Colonna L, *Legal Implications of Data Mining: Assessing the European Union's Data Protection Principles in Light of the United States Government's National Intelligence Data Mining Practices* (PhD thesis, Stockholm University 2016) 193

EU and Canada PNR Agreement Invalid (SCL The IT Law Society 2016), <https:// www.scl.org/news/3734-eu-and-canada-pnr-agreement-invalid>

European Digital Rights (EDRi), 'European Court Opinion: Canada PNR cannot be signed', <https://edri.org/european-court- opinion-canada-pnr-deal-cannot-be-signed/>

Friedman D, *Future Imperfect: Technology and Freedom in an Uncertain World* (Cambridge University Press 2008) 66-79

Hijmans H, 'PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators' (2017) European Data Protection Law Review 310

Hijmans H, *The European Union as a Constitutional Guardian of Internet Privacy and Data Protection: The Story of Article 16 TFEU* (Springer International Publishing 2016) 267

Horowitz S, *'Foucalt's* Panopticon: A Model of NSA Surveillance?' in Russel A. Miller, *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair* (Cambridge University Press2017) 39-62

Hustinx P, 'European Leadership in Privacy and Data Protection' in Artemi Rallo Lombarte and Rosario García Mahamut (eds), *Hacia un nuevo régimen europeo de protección de datos* (Tirant Lo Blanch 2015) 18

Knapp K, 'The Social Construction of Computational Surveillance: Reclaiming Agency in a Computed World' (PhD thesis, London School of Economics and Political Science 2016) 26

Lenaerts K and Van Nuffel P, *European Union Law*, (3rd edn, Sweet & Maxwell 2011) 141

Marx G T, 'Coming to Terms: The Kaleidoscope of Privacy and Surveillance', in Beate Roessler and Dorota Mokrosinska (eds) *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge University Press 2015) 33-34

Miller R A, *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair* (Cambridge University Press 2017)

Monteleone S and Puccio L, *From Safe Harbour to Privacy Shield: Advances and shortcomings of the new EU-US data transfer rules* (European Parliamentary Research Service In-Depth Analysis 2017) 11

Rotenberg M and others, 'Enforcing Privacy Rights: Class Action Litigation and the Challenge of cy pres' in David Wright and Paul de Hert, *Enforcing Privacy. Regulatory, Legal and Technical Approaches* (Springer 2016) 307-334

Sanchez Ferro S, 'The Need for an Institutionalized and Transparent Set of Domestic Legal Rules Governing Transnational Intelligence Sharing in Democratic Societies' in Miller R A, *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair* (Cambridge University Press 2017)

Schuster S (ed.) *Mass Surveillance: Part 1 - Risks and opportunities raised by the current generation of network services and applications* (STOA Report European Parliamentary Research Service, Brussels, 2015) 8

Solove D, *The Digital Person: Technology and privacy in the information age* (NYU Press 2004) 168-180

Stiennon R, *There Will Be Cyberwar: How the Move To Network-Centric War Fighting Has Set The Stage For Cyberwar* (IT-Harvest Press 2015) 67-77

Swire P, 'US Surveillance Law in a constitutional democracy, Safe Harbor, and Reforms since 2013' in Dan Svantesson and Dariusz Kloza (eds), *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy* (Intersentia 2017) 85-126

Taylor M, 'Flying from the EU to the US: necessary extraterritorial legal diffusion in the US-EU Passenger Name Record agreement' (2015) 19 Spanish Yearbook of International Law 223-225

Vermeulen G, 'The Paper Shield. On the degree of protection of the EU-US Privacy Shield against unnecessary or disproportionate data collection by the US intelligence and law enforcement services' in Dan Svantesson and Dariusz Kloza, *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy* (Intersentia 2017) 127-147

Vladeck D, 'Separated by Common Goals: A U.S. Perspective on Narrowing the U.S.-E.U. Privacy Divide' in Lombarte AR and Mahamut RC (eds) *Hacia un nuevo régimen europeo de protección de datos* (Tirant Lo Blanch 2015)

Weiss M A and Archick K, 'U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield, Congressional Research Service report', <https://fas.org/sgp/crs/misc/R44257.pdf>

Wensink W, Warmenhoven B, Haasnoot R et al., 'The European Union's Policies on Counter-Terrorism: Relevance, Coherence and Effectiveness', (Brussels 2017) 121-123 <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/ 583124/IPOL_STU(2017)583124_EN.pdf>

Zedner L, 'Why Blanket Surveillance Is No Security Blanket: Data Retention in the United Kingdom after the European Data Protection Directive' in Miller R A, *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair* (Cambridge University Press 2017) 564-585

Since the Snowden revelations, the adoption in May 2016 of the General Data Protection Regulation and several ground-breaking judgments of the Court of Justice of the European Union, data protection and privacy are high on the agenda of policymakers, industries and the legal research community.

Against this backdrop, *Data Protection and Privacy under Pressure* sheds light on key developments where individuals' rights to data protection and privacy are at stake. The book discusses the persistent transatlantic tensions around various EU-US data transfer mechanisms and EU jurisdiction claims over non-EU-based companies, both sparked by milestone court cases. Additionally, it scrutinises the expanding control or surveillance mechanisms and interconnection of databases in the areas of migration control, internal security and law enforcement, and oversight thereon. Finally, it explores current and future legal challenges related to big data and automated decision-making in the contexts of policing, pharmaceutics and advertising.

Gert Vermeulen is full professor of international and European criminal law and director of the Institute for International Research on Criminal Policy (IRCP) at Ghent University, and privacy commissioner at the Belgian DPA.

Eva Lievens is assistant professor of law and technology at Ghent University.

www.maklu.eu
isbn 978-90-466-0910-1