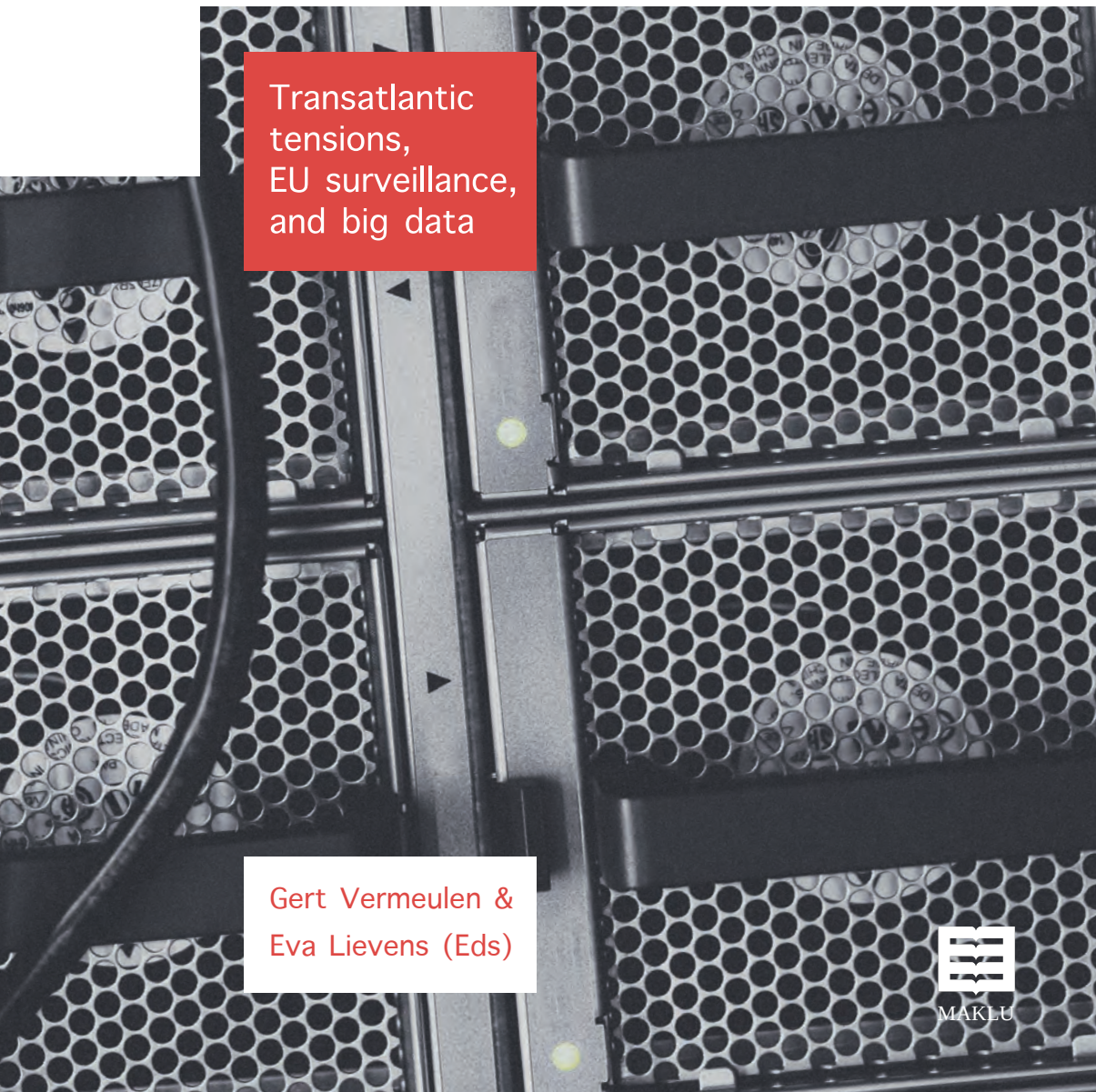
Data Protection and Privacy under Pressure



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

Eyes wide shut

The Privacy Shield's blunt denial of continued bulk, mass or indiscriminate collection or processing and unnecessary or disproportionate access and use by US intelligence and law enforcement authorities

GERT VERMEULEN[1]

1. INADEQUACY OF THE US DATA PROTECTION REGIME: CLEAR SINCE 9/11, CLEARER SINCE SNOWDEN

The Europol-US agreement of 20 December 2002[2] and the EU-US mutual assistance treaty in criminal matters of 25 June 2003[3], both concluded in the immediate aftermath of 9/11, soon set the tone, in that US non-compliance with key EU data protection standards was set aside in favour of enabling EU-US data flows after all.

[1] Full Professor of International and European Criminal Law, Director Institute for International Research on Criminal Policy (IRCP), Department Chair Criminology, Criminal Law and Social Law, Faculty of Law, Ghent University; Privacy Commissioner, Commission for the Protection of Privacy (Belgium). Email: gert.vermeulen@ugent.be. This text is an updated and elaborate version of 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 JB Svantesson and Dariusz Kloza (eds), *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy* (European Integration and Democracy Series, vol 4, Intersentia 2017).

[2] Supplemental agreement on the exchange of personal data and related information (Europol Police Office-United States of America) (20 December 2002) <https://www.europol.europa.eu/content/supplemental-agreement-between-europol-police-office-and-united-states-america>

[3] Agreement on mutual legal assistance (European Union-United States of America) (25 June 2003) OJ L 181/34.

Neither in terms of police or judicial cooperation the adequacy of the US data protection level could be established, whilst both the (then) Europol-Agreement and Directive 95/46[4] required so. Purpose limitation (specialty)[5] in the use of data provided by Europol or EU Member States proved an almost nugatory concept, where the US was allowed to freely make use of information that was procured in criminal cases for purely administrative or intelligence purposes.[6] Later, in 2006, it was revealed that the US Treasury had procured access to worldwide scriptural bank transactions by means of administrative subpoenas *vis-à-vis* the US hub of the (Belgium-based) *Society for Worldwide Interbank Financial Telecommunication* (SWIFT) in the context of combating the financing of terrorism, but surely alluding to other (including economic) goals as well.[7] Moreover, SWIFT itself defected herein, as its US hub did not endorse the so-called *Safe Harbour* principles.[8] These had been developed in 2000 by the European Commission[9] to ensure that, given that the US data

[4] Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.

[5] Els De Busser, 'Purpose limitation in EU-US data exchange in criminal matters: the remains of the day' in Marc Cools and others (eds), *Readings on criminal justice, criminal law and policing* (Vol 2, Maklu 2009) 163.

[6] Steve Peers, 'The exchange of personal data between Europol and the USA' (2003) Statewatch Analysis no 15 <www.statewatch.org>; Gert Vermeulen, 'Transatlantisch monsterverbond of verstandshuwelijk? Over het verschil tussen oorlog en juridische strijd tegen terreur en de versterkte politie- en justitiesamenwerking tussen EU en VS' (2004) 25(1) Panopticon 90; Paul De Hert and Bart De Schutter, 'International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and Swift' in Bernd Martenczuk and Servaas Van Thiel (eds), *Justice, Liberty, Security: New Challenges for EU External Relations* (I.E.S. series nr. 11, VUB Press 2008) 326-327 and 329-333.

[7] See Belgian Privacy Commission, 'Opinion on the Transfer of Personal Data by the CSLR SWIFT by Virtue of UST (OFAC)' 37/2006 <https://www.privacycommission.be/sites/privacycommission/files/documents/advies_37_2006_1.pdf>; Also: Patrick M Connorton, 'Tracking Terrorist Financing through SWIFT: When U.S. subpoenas and foreign privacy law collide' (2007) 76(1) Fordham L Rev 283.

[8] Gloria González Fuster, Paul De Hert and Serge Gutwirth, 'SWIFT and the vulnerability of transatlantic data transfers' (2008) 22(1-2) Intl Rev of L Computers & Technology 191.

[9] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L 215/7.

protection regime in itself could not be qualified as adequate, commercial EU-US data transfers would nonetheless be enabled.[10] Companies that indicated (and self-certified) their compliance with the principles laid down in the Commission's Safe Harbour Decision, were to be considered as – from a data protection perspective – 'safe harbours' within US territory, to which EU companies were allowed to transfer data. This, however, was not the case for the SWIFT hub in the US, so that the Belgian company should have refrained from localizing (backup) data in it. The EU's response to this scandal was far from convincing. While intra-European payment transactions were admittedly no longer sent to the US hub (albeit that in the meantime SWIFT had registered it as a 'safe harbour'), the Commission negotiated on behalf of the EU an agreement with the US, allowing the latter, via a Europol 'filter' (which painfully lacks proper filtering capacity) to obtain *bulk*-access on a case-by-case basis to these intra-European payment transactions. This 2010 TFTP-agreement (*Terrorist Financing Tracking Program*[11]) furthermore contains an article in which the US Treasury is axiomatically deemed adequate in terms of data protection.[12] Notwithstanding this, and given the known practice of wide data-sharing between US government administrations and bodies contrary to the European purpose-limitation principle, the *in*adequacy of the US data protection regime was at the time beyond doubt. That the Foreign Intelligence Surveillance Act (FISA)[13], amended post-9/11 with the Patriot Act[14] and further expanded in 2008[15] (FISA Amendments Act), allowed the US to monitor – either with or without a court order – electronic communication in

---

[10] See William J Long and Marc Pang Quek, 'Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise' (2002) 9(3) JEPP 325.

[11]Agreement on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program (European Union–United States of America) (30 November 2009) OJ L 008/11.

[12] Article 6 of the TFTP Agreement (n 11) reads: " […] the U.S. Treasury Department is deemed to ensure an adequate level of data protection for the processing of financial payment messaging and related data transferred from the European Union to the United States for purposes of this Agreement."

[13] Foreign Intelligence Surveillance Act of 1978 50 USC §§ 1801-11, 1821-29, 1841-46, 1861-62, 1871.

[14] Uniting and Strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) Act of 2001; Paul T Jaeger, John Carlo Bertot and Charles R McClure, 'The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act' (2003) 20 Government Information Quarterly 295.

[15] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008.

a way that was disproportionate, worldwide and in bulk, was clear as well.[16] This and more was confirmed in the summer of 2013 with the revelations of whistleblower *Edward Snowden.* [17] These revelations were particularly shocking because of the revealed extent of the interception practices of the NSA (National Security Agency) – *inter alia* through the PRISM and Upstream programmes – and the British intelligence service GCHQ's (Government Communications Headquarters)[18] – which for years had spied on *Belgacom International Carrier Service* (Bics). As a subsidiary of Belgium-based (tele)communications provider *Proximus*, Bics provides worldwide hardware through which telecom companies and government agencies run their electronic communication (internet-, telephony-, mobile- and texting-traffic). Moreover, the intense mutual cooperation between the NSA and GCHQ, and within the so-called Five Eyes Community (comprising the intelligence services of Canada, Australia and New Zealand), was confirmed by the revelations, although many were well aware that these five, within the context of Echelon, had been monitoring worldwide satellite communications for decades, including for commercial purposes. Already in 2000, the European Parliament had instigated an investigative commission against these practices.[19] From the US

---

[16] Els De Busser, 'Purpose limitation in EU-US data exchange in criminal matters: the remains of the day' in Marc Cools and others (eds), *Readings on criminal justice, criminal law and policing* (Vol 2, Maklu 2009) 163; Els De Busser, *Data Protection in EU and US Criminal Cooperation* (Maklu 2009).

[17] The outrage broke in June 2013, when *the Guardian* first reported that the US National Security Agency (NSA) was collecting the telephone records of tens of millions of Americans, see: Glenn Greenwald, 'NSA collecting phone records of millions of Verizon customers daily' *The Guardian* (London, 6 June 2013) <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>; Also: Mary-Rose Papandrea, 'Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment' (2014) 94(2) Boston U L Rev 449.

[18] The involvement of the British GCHQ was revealed by *the Guardian* on the 21st of June, 2013. See: Ewen MacAskill and others, 'GCHQ taps fibre-optic cables for secret access to world's communications' *The Guardian*, (London, 21 June 2013) <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>.

[19] See European Parliament decision setting up a temporary committee on the ECHELON interception system, 29 June 2000 <http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=B5-2000-0593&language=EN> and the final report that was published in 2001: Temporary Committee on the ECHELON Interception System, 'Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))' FINAL A5-0264/2001 PAR1, 11 July 2001. See also: Franco Piodi and Lolanda Mombelli, 'The ECHELON Affair. The European Parliament and the Global Interception System

side, the publication of NSA-newsletters in the summer of 2015 as a result of the *Snowden* revelations, plainly confirmed these allegations.[20]

2. SAFE HARBOUR DEAD

Using the leverage handed to her under the Lisbon Treaty[21], the then Commissioner of Justice *Reding* launched an ambitious legislative data protection package at the outset of 2012.[22] A proposed regulation was initiated to replace Directive 95/46[23] , and aimed *inter alia* to bind (US) service providers on EU territory by European rules on data protection. In parallel, a proposed directive had to upgrade the 2008 Framework Decision on data protection in the sphere of police and judicial cooperation in criminal matters.[24] In Decem-

1998 – 2002' (2014) European Parliament History Series <http://www.europarl.europa.eu/EPRS/EPRS_STUDY_538877_AffaireEchelon-EN.pdf>.

[20] See Henry Farrell and Abraham Newman, 'Transatlantic Data War. Europe fights back against the NSA' (2016) 95(1) Foreign Affairs 124.

[21] Treaty of Lisbon Amending the Treaty on European Union and the Treaty establishing the European Community (adopted 17 December 2007) OJ 2007/C 306/01.

[22] Viviane Reding, 'The European data protection framework for the twenty-first century' (2012) 2(3) International Data Privacy Law 119; Commission, 'Safeguarding Privacy in a Connected World -A European Data Protection Framework for the 21st Century' (Communication) COM (2012) 9 final.

[23] Colin J Bennet and Charles D Raab, 'The Adequacy of Privacy: the European Union Data Protection Directive and the North American Response' (1997) 13 The Information Society 245, 252.

[24] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L 350/60; See also: Els De Busser and Gert Vermeulen, 'Towards a coherent EU policy on outgoing data transfers for use in criminal matters? The adequacy requirement and the framework decision on data protection in criminal matters. A transatlantic exercise in adequacy' in Marc Cools and others (eds), *EU and International Crime Control* (vol 4, Maklu 2010).

ber 2015 political agreement was reached on the new Regulation and the Directive.[25] Both of them were formally adopted in April 2016[26] and EU Member States are due to apply them from 25 respectively 6 May 2018 onwards. The adequacy requirement for data transfers to third states moreover remains intact. *Reding* also took up the defense for EU citizens for what concerns US access to their personal data.[27] Just a few months after the *Snowden* revelations, she came up with two parallel communications at the end of November 2013: 'Rebuilding Trust in EU-US Data Flows' (COM(2013) 846 final)[28] and 'communication on the functioning of the Safe Harbour from the perspective of EU citizens and companies established in the EU' (COM(2013) 847 final)[29] (hereafter: Safe Harbour communication). The first communication was accompanied by a report containing the 'findings on the ad-hoc workgroup data protection of the EU and the US'[30], which, among others, stipulated that the improvements in the Safe Harbour Decision should address the 'structural deficiencies in relation to the transparency and enforcement, the material safe harbour principles and the functioning of the *exception for*

---

[25] For an overview of the route leading up to these instruments, see the (then: 2004-2014) European Data Protection Supervisor's overview: Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' (2015) <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf>.

[26] Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1; Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89.

[27] See Els De Busser, 'Privatization of Information and the Data Protection Reform' in Serge Gutwirth and others (eds), *Reloading Data Protection* (Springer 2014).

[28] Commission, 'Rebuilding Trust in EU-US Data Flows' (Communication) COM(2013) 846 final.

[29] Commission, 'Communication on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU' (Communication) COM(2013) 847 final.

[30] Report of 27 November 2013 on the Findings by the EU Co-Chairs of the Ad Hoc EU-US Working Group on Data Protection [2013] <http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf>.

national security'.[31] After all, the Safe Harbour Decision explicitly determined that the demands of 'national security, public interest and law enforcement' of the US supersede the Safe Harbour principles.[32] As it turned out, these exceptions rendered the safe harbours unsafe. In its 2013 Safe Harbour communication, the Commission established that 'all companies involved in the PRISM-programme, and which grant access to US authorities to data stored and processed in the US, appear to be Safe Harbour certified.' As such, '[t]his has made the Safe Harbour scheme one of the conduits through which access is given to US intelligence authorities to collecting personal data initially processed in the EU' (point 7). This was indeed the case: *Microsoft, Google, Facebook, Apple, Yahoo!, Skype, YouTube* … all of them were self-certified under Safe Harbour and simultaneously involved in the PRISM-programme. The Commission concluded that '[t]he large scale nature of these programmes may [have] result[ed] in [*more*] data transferred under Safe Harbour being accessed and further processed by US authorities *beyond what is strictly necessary and proportionate to the protection of national security* as foreseen under the exception provided in the Safe Harbour Decision'.[33]

Real urgency in the negotiations with the US only (re)surfaced following the ruling of the CJEU on 6 October 2015 in response to the appeal of *Max Schrems* against the Irish Data Protection Commissioner (in proceedings against *Facebook*[34], that has its European headquarters in Dublin) before the Irish High Court.[35] The latter had requested a preliminary ruling by the CJEU, namely as to whether the Irish privacy commissioner (as it had itself upheld) was bound by the Safe Harbour Decision of the Commission to the extent that it could no longer be questioned whether the US data protection regime was adequate, as such leading the Irish privacy commissioner to conclude that it could not investigate the complaint filed by *Schrems*. The latter had argued the contrary, based on the post-*Snowden* ascertainment that *Facebook* was active in the PRISM-programme, regardless of its self-certification under the Safe Harbour principles.[36] The CJEU concluded *inter alia* that '[t]he right to respect for

---

[31] Emphasis added.

[32] See Annex I, para 4.

[33] Safe Harbour Communication (n 29) point 7.1. (emphasis added).

[34] Natasha Simmons, 'Facebook and the Privacy Frontier' (2012) 33(3) JBL 58.

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

[36] Andreas Kirchner, 'Reflections on privacy in the age of global electronic data processing with a focus on data processing practices of facebook' (2012) 6(1) Masaryk University Journal of Law and Technology 73; Mireille Hildebrandt, 'The rule of law in

private life, guaranteed by article 7 of the Charter and by the core values common to the traditions of the Member States, would be rendered meaningless if the State authorities were authorised to access electronic communications on a casual and generalised basis without any objective justification based on *considerations of national security or the prevention of crime that are specific to the individual concerned and without those practices being accompanied by appropriate and verifiable safeguards*'.[37] The CJEU furthermore recalled, with explicit reference to its Data Retention judgment of 8 April 2014[38] (in which it had declared the Data Retention Directive invalid) and its earlier judgments as cited under points 54 & 55 of its Data Retention judgment, its consistent case-law that 'EU legislation involving interference with the fundamental rights guaranteed by articles 7 and 8 of the Charter [regarding the respect for private and family life and the protection of personal data respectively] must, according to the Court's settled case-law, lay down *clear and precise* rules governing the scope and application of a measure […]'.[39] Still with reference to the Data Retention judgment (and the case-law cited under point 52 hereof), the CJEU jointly stated that 'furthermore and above all, protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply *only in so far as is strictly necessary*'[40], whereby of course '[l]egislation *is not*

cyberspace?' (Inaugural Lecture at Radboud University Nijmegen, 2013) <http://works.bepress.com/mireille_hildebrandt/48/>; Bert-Jaap Koops, 'The trouble with European data protection law' (2014) Tilburg Law School Legal Studies Research Paper Series 04/2015 <http://m.isaca. org/Groups/Professional-English/privacy-data-protection/GroupDocuments/2014-08-24%20%20The%20Trouble%20with%20European%20Data%20Protection%20 Law.pdf>; Fanny Coudert, 'Schrems vs. Data Protection Commissioner: a slap on the wrist for the Commission and new powers for data protection authorities' (*European Law Blog* 2015) <https://lirias.kuleuven.be/bitstream/123456789/511500/1/FannyCoudert_Post+CJEU+Schrems_final.pdf>; Reid Day, 'Let the magistrates revolt: A review of search warrant applications for electronic in-formation possessed by online services' (2015) 64(2) U Kan L Rev 491; Shane Darcy, 'Battling for the Rights to Privacy and Data Protection in the Irish Courts' (2015) 31(80) Utrecht J of Intl and Eur L 131; David Flint, 'Computers and internet: Sunk without a trace – the demise of safe harbor' (2015) 36(6) JBL 236; Hannah Crowther, 'Invalidity of the US Safe Harbor framework: what does it mean?' (2016) 11(2) JIPLP 88; Nora Ni Loideain, 'The End of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law' (2016) 19(8) J Internet L 7.

[37] *Maximillian Schrems* (n 34) para 34 (emphasis added).

[38] Joined Cases C 293/12 and C 594/12 *Digital Rights Ireland a.o.* EU:C:2014:238.

[39] *Maximillian Schrems* (n 34) para 91 (emphasis added).

[40] ibid, para 92 (emphasis added).

limited to what is strictly necessary where it authorises, on a generalised basis, *storage* of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in 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'.[41] In other words: collection (storage), access and use for reasons of national security, public interest or law enforcement require *specific and precise* criteria and are but allowed when *strictly necessary for specific purposes that are strictly restricted*. Given the fact that the Commission had omitted to implement such an assessment in its Safe Harbour Decision, the CJEU decided on the invalidity of the latter. Hence, with the *Schrems* case, the CJEU firmly put the finger on the following issue: engagements by US companies through self-certification under the Safe Harbour principles do not provide (adequate) protection as long as it remains unclear whether, despite large-scale interception programmes like PRISM, the US privacy regime may be considered adequate. With the sudden invalidity of the Safe Harbour Decision, a replacement instrument became an urgent necessity. The European Commission (since November 2014 the *Juncker* Commission, with *Věra Jourová* as the Commissioner for justice, fundamental rights and citizenship competent *inter alia* for data protection, under custody of super-commissioner (vice-president of the Commission) *Frans Timmermans* was quick to temper emotions. In a communication on the very day of the CJEU's decision, *Timmermans* recognized the Court's confirmation of the necessity 'of having robust data protection safeguards in place before transferring citizens' data'. He furthermore added that, following its Safe Harbour communication, the Commission was working with the US authorities 'to make data transfers *safer* for European citizens' and that, in light of the *Schrems* judgment, it would continue to work 'towards a renewed and *safe* framework for the transfer of personal data across the Atlantic'.[42]

---

[41] ibid, para 93 (emphasis added).

[42] Commission, 'Communication on the transfer of personal data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)' (Communication) COM(2015) 566 final; First Vice-President Timmermans and Commissioner Jourová, 'Press conference on Safe Harbour following the Court ruling in case C-362/14 (Schrems)' (Statement European Commission, 6 October 2015) (emphasis added).

3. LONG LIVE THE PRIVACY SHIELD? *TELE2 SVERIGE AB* AND DIGITAL RIGHTS IRELAND RESPECTIVELY *LA QUADRATURE DU NET* AND OTHERS V COMMISSION

On 29 February 2016, the Commission presented its eagerly awaited 'solution'. It launched a new communication, 'Transatlantic Data Flows: Restoring Trust through Strong Safeguards'[43], and immediately attached hereto – in replacement of the invalidated Safe Harbour Decision – its draft adequacy decision[44] of the US data protection regime (with 7 annexes) for data transfers under the protection of the so-called 'EU-US Privacy Shield'. On the JHA Council the day after, Jourovà hooted: 'Written assurances regarding the limitations on access to data by US public authorities on national security grounds'. Following a negative initial opinion about the initial draft decision, issued by the Article 29 Data Protection Working Party on 13 April 2016,[45] the Commission had no viable choice but to initiate summary renegotiations with the US, leading to just marginal adjustments of the Privacy Shield. The Article 29 Working Party (having nothing but mere advisory power in the first place) gave in,[46] as did the Article 31 Committee[47] (which did have veto power over the draft decision). The revised version of the Privacy Shield adequacy decision was adopted by the European Commission on 12 July 2016.

Un-surprisingly, the Privacy Shield is already facing legal challenges before the CJEU, following two actions for annulment filed on 16 September and 25 October 2016 in cases brought by Digital Rights Ireland[48] respectively *La Quadrature du Net* and Others[49] against the Commission, which the below

---

[43] Commission, 'Transatlantic Data Flows: Restoring Trust through Strong Safeguards' (Communication) COM(2016) 117 final.

[44] Commission Implementing Decision of xxx pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield.

[45] Article 29 Working Party, 'Press release' (13 April 2016); Article 29 Working Party, 'Opinion 01/2016 on the draft EU-U.S. Privacy Shield adequacy decision' WP 238 (13 April 2016).

[46] Article 29 Working Party, 'Press release' (1 July 2016).

[47] On 8 July 2016, following its non-decision of 19 May on the initial version of the Privacy Shield.

[48] Case T-670/16 *Digital Rights Ireland v Commission* [2016] action brought on September 16, 2016.

[49] Case T-738/16 *La Quadrature du Net and Others v Commission* [2016] action brought on October 25, 2016.

analysis will refer to where relevant.[50] This will equally be the case for the Irish High Court judgment of 3 October 2017 in the case between *the Irish Data Protection Commissioner v Facebook Ireland Ltd.* and *Maximillian Schrems*, referring the issue of the validity of the Standard Contractual Clauses underlying personal data transfers from Facebook Ireland to Facebook Inc. (US) to the CJEU for a preliminary ruling.[51] At least indirectly, the case surely adds to the pressure on the Privacy Shield as well. Even with over 2,500 companies[52] self-certified under the new scheme, it will likely not survive infancy.

This is especially true since the CJEU has issued yet another judgment, on 21 December 2016, after a request for a preliminary ruling in the case *Tele2 Sverige AB*,[53] on data retention under the ePrivacy Directive. As will be explained in the analysis below, the findings of the CJEU at least indirectly place a bomb under the Privacy Shield as well, where it holds that 'general and indiscriminate retention of traffic data and location data' is inacceptable, leaving Member States the possibility for only 'targeted'[54] retention of traffic and location data, meaning that such retention must then be defined also in terms of the 'public […] that may potentially be affected'[55] and on the basis of 'objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security'[56]. Indiscriminate data collection, irrespective of later access or use restrictions, has been formally invalidated by the CJEU,

---

[50] Leaving out pleas and arguments relating to a lack of effective remedy or provision of independent monitoring under the Privacy Shield or US law, since these are not the focuses of the current contribution.

[51] *The Data Protection Commissioner v Facebook Ireland Limited And Maximillian Schrems* (2016) No. 4809 P. (The Hight Court Commercial) <http://www.europe-v-facebook.org/sh2/HCJ.pdf>. Reference to this judgment will also remain limited, ie by not dealing with the core issue of lack of effective remedy under the Standard Contractual Clauses transfer mechanism.

[52] The International Trade Administration (ITA) US Department of Commerce, 'Privacy Shield List' <https://www.privacyshield.gov/list>.

[53] 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 Tom Watson* EU:C:2016:970.

[54] ibid, para 108.

[55] ibid, paras 110-111.

[56] ibid, para 111.

even in a clearer fashion than in its 2014 Data Retention judgment. Interestingly, it has moreover explicitly ruled that data concerned must be retained within the European Union, which indirectly raises fresh doubts about the legitimacy of transferring (electronic communications) data under the Privacy Shield, and even under the Umbrella Agreement or the TFTP.

Before evaluating the Privacy Shield on its merits, it pays to bear in mind that, conceptually, it bears a very strong resemblance with the Safe Harbour regime. The *Safe Harbour* principles have now been renamed as *privacy* principles, which should serve as the new basis for data transfers coming from the EU to organizations – essentially: corporations – in the US who endorse these principles through the act of self-certification. Mirroring the Safe Harbour Decision, there is furthermore a general exception hereto should national security, public interest or law enforcement require so. Hence, the central question is whether the 'limitations' and 'safeguards' that are presented by the Privacy Shield – the Safe Harbour regime did not foresee any of these – are convincing enough. The way in which the European Commission desperately tried to convince everyone, through the means of its communication and the attached (draft) adequacy decision, of the satisfactory nature of the new regime, and that the US will effectively display an adequate data protection level under the Privacy Shield, is painful to witness. The heydays of former European justice commissioner *Reding* seem long gone. Apparently, demanding a genuine commitment of the US to refrain from collecting in bulk personal data of EU citizens or coming from the EU, and to only intercept communications and other personal data when strictly necessary and proportionate, was a political bridge too far. It seems that Commissioner *Jourová* (and super-commissioner *Timmermans*) have succumbed to the dominant importance of maintaining benevolent trans-Atlantic trade relations. Allowing trans-Atlantic transfers of personal data from companies or their subsidiaries in the EU to companies based in the US is after all the primordial goal of the Privacy Shield. Tough negotiating was apparently not considered an option, not even in the renegotiation stage. Nonetheless, one fails to see why such a commercial transfer of personal data *without* the option to do so in bulk, or without resorting to a capturing of such data that is disproportionate for intelligence or law enforcement purposes, would have been too high of a stake during negotiations. Companies - including the major US players like *Google, Apple, Facebook and Microsoft* - will *in the long run* not benefit from the fact that they will not be able to protect the data of their European or other users against government access. It is regrettable that they themselves seem insufficiently aware of this, leaving aside scarce counter-examples like the Apple-FBI

clash.[57] In the meantime, the very minimum is to burst the bubble of the European Commission's discourse in the privacy shield communication and its (draft) adequacy decision. The 'limitations' and 'safeguards' that the shield - according to the Commission - offers against US data collection in the interest of national security (by the intelligence services), public interest or law enforcement (by the police) are by absolutely no means sufficient. A simple focused reading and concise analysis hereof suffice to demonstrate this.

4. DATA COLLECTION FOR NATIONAL SECURITY PURPOSES

4.1. Amalgamation of collection and access v access and use

The Commission's analysis is misleading because it repeatedly posits that the 'limitations' to which the US will commit and that are applicable on the parts concerning 'access' and 'use'[58] for the purpose of national security, public interest or law enforcement, will be sufficient in light of EU law to amount to an adequate level of data protection. According to EU law, however, processing of personal data takes place as soon as 'collection' takes place, regardless of any future 'access' to this data or the 'use' thereof. By systematically wielding the term 'access' instead of 'collection', or by posing as if the limitations regarding 'access' will - with the proverbial single stroke of a brush - also include sufficient limitations in terms of 'collection', the Commission is wilfully pulling one's leg. To the extent still necessary, it suffices to recall the previously mentioned 2014 Data Retention judgment of the CJEU. In the latter, the Court abundantly made clear that limitations are necessary both in the phase of the 'collection' of personal data (*in casu* retention or conservation by suppliers of electronic communication services of traffic data in fixed and mobile telephony, internet access, internet e-mail and internet telephony) as in the phases of 'accessing' this data or its later 'use' (*in casu* by the competent police and judicial authorities). As such, the Commission skips a step, or at least tries to maintain the illusion that the Privacy Shield's limitations in terms of 'access' and 'use' will suffice to speak of an adequate data protection. This, however, is a flagrantly false rhetoric. Just the same, also the part that concerns the initial 'collection' of personal data by the competent authorities (*in*

[57] See, eg X, 'Taking a bite at the Apple. The FBI's legal battle with the maker of iPhones is an escalation of a long-simmering conflict about encryption and security' *The Economist* (London, 27 February 2016) <http://www.economist.com/news/science-and-technology/21693564-fbis-legal-battle-maker-iphones-escalation>.

[58] Commission Implementing Decision of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield [2016] C(2016) 4176 final (revised decision) para 67.

casu the US intelligence or law enforcement services) is bound by strict requirements. After all, one of the reasons why the CJEU dismissed the Data Retention Directive as invalid[59] was because 'in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences'. It is important to bear in mind that back then, the debate was only on the conservation (and as such 'collection') by service providers of electronic communications, and not even on the direct 'collection' by intelligence and law enforcement services themselves, as is currently the case with the Privacy Shield.

With the CJEU judgment in *Tele2 Sverige AB* of December 2016, there is no doubt left that any preventative data retention must be 'limited […] to what is strictly necessary', 'with respect to the categories of data to be retained, the means of communication affected, *the persons concerned* and the retention period adopted',[60] these limitation criteria being explicitly cumulative, whilst the initial Data Retention judgment of 2014 (by the use of 'and/or') still left the door open for data retention which would not be targeted in terms of the 'persons concerned' or the 'public affected'.

Apart from this, the CJEU, in its 2014 Data Retention judgment, argued that in the Data Retention Directive '[there is] not only […] a general absence of limits', and that '[it] also fails to lay down any objective criterion by which to determine the limits of the *access* of the competent national authorities to the data and their subsequent *use* for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference'.[61] The Court continued that the 'Directive does not contain substantive and procedural conditions relating to the *access* of the competent national authorities to the data and to their subsequent *use*. Article 4 of the directive, which governs the *access* of those authorities to the data retained, does not expressly provide that that *access* and the subsequent *use* of the data in question must be *strictly restricted* to the purpose of preventing and detecting *precisely defined* serious offences or of conducting

[59] Joined Cases C-293/12 and C 594/12 *Digital Rights Ireland a.o.* EU:C: 2014:238, para 59.

[60] *Tele2* (n 52) para 108 (emphasis added).

[61] *Digital Rights Ireland* (n 59) para 60.

criminal prosecutions relating thereto; it merely provides that each Member State is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements'.[62] Ultimately, and still with reference to 'access' and 'use', the Court lamented that the Directive 'does not lay down any objective criterion by which the number of persons authorised to *access* and *subsequently use* the data retained is limited to what is strictly necessary in the light of the objective pursued' and that '[a]bove all, the access by the competent national authorities to the data retained is not 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. Nor does it lay down a specific obligation on Member States designed to establish such limits'.[63] *Mutatus mutandis*[64] both the necessity and proportionality requirements can be firmly derived from the Data Retention judgment, and this with regards to the 'collection' of data on the one hand, and the 'access' to and 'use' of this data on the other. It was (as a minimum) to be expected from the Commission's Privacy Shield-communication that it would, for the discerned phases of 'collection' and 'access and use' respectively, carefully and systematically inquire into the US-proposed 'limitations' to its processing of and interference with EU personal data, drawing on the EU privacy requirements like these had been operationalized by the CJEU in its 2014 Data Retention judgment. Unfortunately, The privacy Shield Communications does not do so. From a substantive perspective, it is moreover the case that the guarantees in terms of 'collection' are clearly insufficient, since eg bulk collection of data remains perfectly possible under certain scenario's. Not only - and contrary to how it is presented by the Commission - does the Privacy Shield fail to solve this with the limitations it contains in terms of 'access and use', these limitations are inherently flawed as well, as they do not comply with nor mirror the (EU) requirements of strict necessity and proportionality.

---

[62] ibid, para 61 (emphasis added).

[63] ibid, para 62 (emphasis added).

[64] In the context of the Privacy Shield it is not just about the collection of, access to and use of personal data by police and judicial authorities in the framework of serious criminal offences, but also by intelligence and law enforcement services in the context of national security, public interest and law enforcement.

4.2. **Continued bulk or indiscriminate collection and processing**

In itself[65] it is gratifying that under PPD-28 (the *Presidential Policy Directive* 28 of 17 January 2014)[66] intelligence operations concerning sigint (signals intelligence, or the interception of electronic communication) will from now on only be allowed for purposes of foreign or counter-*intelligence* in support of *government* missions, and no longer with a view to benefit US companies' commercial interests. Sigint for industrial espionage, or to allow US companies to poach orders from European counterparts - which, as it turned out, happened *inter alia* with Echelon - has now been prohibited.

As far as diversions go, this is a big one. Following the *Schrems* judgment, this is evidently no longer the issue. The real question is whether the limitations on data collection for government purposes in the fields of national security, public interest (other than for economic motives or to gain a competitive advantage) or law enforcement are convincing enough. The reality is they are not, regardless of the Commission's attempts to mask this. Yet, on the other hand, what we do get is an abundance of vague engagements on behalf of the US. The following is an anthology:

Data collection under PPD-28 shall always be 'as tailored as feasible'[67], and members of the intelligence community '*should* require that, *wherever practicable*, collection *should* be focused on specific foreign intelligence targets or topics *through the use of discriminants* (eg specific facilities, selection terms and identifiers') [68]. There is a little too much of 'should' in this sentence for it to be genuinely convincing. Also, '*wherever practicable*' is both very conditional and open-ended, and the mere use of 'discriminants' evidently does not guarantee compliance with strict necessity and proportionality requirements. At the very most, they imply that bulk collection will not take place without at least some form of selection. Furthermore, the US engagements coming from the Office of the Director of National Intelligence (ODNI) recognise without much ado that bulk-sigint under 'certain' circumstances (that

[65] Commission Implementing Decision (draft decision) (n 43) para 70.

[66] Presidential Policy Directive, 'Signals Intelligence Activities' Presidential policy directive/PPD-28, 17 January 2014 <https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>.

[67] Commission Implementing Decision of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield [2016] C(2016) 4176 final (revised decision) para 71.

[68] ibid, para 70 (emphasis added).

are not very 'certain' to begin with, 'for instance in order to identify and assess new or emerging threats')[69] will still take place. The Commission on its part apparently considers it sufficiently reassuring that this may only take place when targeted collection through the use of discriminants is not deemed feasible 'due to technical or operational reasons'. The recognition by the Commission (dexterously stashed away in footnote 71) that the feasibility report, which was supposed to be presented to former President Obama by the Director of National Intelligence with reference to the possibility of developing software that would make it easier for the intelligence community to '*rather* conduct targeted instead of bulk-collection' [emphasis added], concluded that there is *no* software-based alternative to replace bulk-collection entirely, apparently does not contradict this reasoning. On the contrary, the Commission smoothly falls in with the ODNI's own estimation that bulk collection will not be the rule (rather than the exception)[70] - as if that would be sufficient in light of the EU requirements in terms of collection. Similarly comforting to the Commission is that the assessment of when a more targeted collection would be deemed technically or operationally 'not feasible', is not left to the individual discretion of individual staff of the intelligence community.[71] Now that really would have been quite wrong. In addition, the Commission sees an extra 'safeguard' in the fact that the potential 'discriminants' shall be determined by high-level policy makers, and that they will be (re)evaluated on a regular basis.[72] Ultimately, the Commission seems fully convinced when the ODNI-engagements make it clear that bulk-sigint *use* will - in any case - remain 'limited' to a list of six 'specific' national security purposes (cf. below, under c.). Limitations to the phase of 'use' do not, however, imply safeguards to the phase of 'collection'. This is rather *basic* in EU privacy law. To sum it up in the Commission's own view, the conclusion is that '*although not phrased in those legal terms'*, there is compliance with the EU requirements of necessity and proportionality[73]: bulk-collection needs to remain the exception rather than the rule, and should it nevertheless take place, the six 'strict' limitations for *use* are applicable. Rephrased in non-misleading terms: bulk-collection remains possible, so that it is by no means compliant with the tight restrictions of EU privacy law in terms of data collection.

---

[69] ibid, para 72.

[70] ibid, para 71.

[71] Commission Implementing Decision (draft decision) (n 43) para 60; more broadly phrased in Commission Implementing Decision (revised decision) para 70.

[72] Commission Implementing Decision (revised decision) (n 64) para 70.

[73] ibid, para 76.

The above argumentation is also prominently featuring in the actions for annulment of the Commission's Privacy Shield adequacy decision brought in the fall of 2016 by Digital Rights Ireland respectively *La Quadrature du Net* and Others. The 4th plea in law relied on by Digital Rights Ireland alleges that the provisions of the FISA Amendments Act 'constitute legislation permitting public authorities to have *access on a generalised basis* to the content of electronic communications and consequently are not concordant with Article 7 of the Charter […]'[74]. The generalised nature of collections allowed under the US regulatory regime is also the core element underlying the 1st plea in law put forward by *La Quadrature du Net* and Others,[75] leading them to conclude that the adequacy decision infringes article 7 of the Charter by not drawing the conclusion that such 'access on a generalised basis to the content of electronic communications' compromises the essence of the fundamental right to respect for private life. The plea in law draws on several paragraphs of the revised decision itself: '[…] PPD-28 explains that Intelligence Community elements *must sometimes collect bulk signals intelligence* in certain circumstances, for instance in order to identify and assess new or emerging threats […]'[76]; 'According to the representations from the ODNI, even *where the Intelligence Community cannot use specific identifiers to target collection*, it will seek to narrow the collection 'as much as possible' […]'[77]; '[…] Targeted collection is clearly prioritised, while *bulk collection is limited to (exceptional) situations* where targeted collection is not possible for technical or operational reasons. […]'[78].

To the extent necessary, also the Irish High Court, in its judgment of 3 October 2017[79], unambiguously established that '[o]n the basis of [the] definition [in Directive 95/46] and the evidence in relation to the operation of the PRISM and Upstream programmes authorised under s. 702 of FISA, it is clear that there is *mass indiscriminate processing* of data by the Unites States government agencies, whether this is described as mass or targeted surveillance'.

---

[74] Case T-670/16 *Digital Rights Ireland v Commission* [2016] action brought on September 16, 2016 (emphasis added).

[75] Case T-738/16 *La Quadrature du Net and Others v Commission* [2016] action brought on October 25, 2016.

[76] Commission Implementing Decision (revised decision) (n 64) para 72 (emphasis added).

[77] ibid, para 73 (emphasis added).

[78] ibid, para 76 (emphasis added).

[79] *The Data Protection Commissioner v Facebook Ireland Limited And Maximillian Schrems* (n 50) para 193 (emphasis added).

Even if, for Upstream, it may well be the case that 'mass *searching* […] is for targeted communications and […] in that sense not indiscriminate, […] it involves the *collection* of non-relevant data […]', so the Court held, thereby confirming the essential difference between 'bulk *searching*' v 'bulk *acquisition, collection or retention*'[80].

4.3. Access and use beyond strict necessity and proportionality

The six 'specific' national security purposes (mentioned above) to which the bulk-sigint *use* will be 'limited' according to the ODNI-engagements are the following[81]: 'detecting and countering certain activities of foreign powers, counterterrorism, counter-proliferation, cybersecurity, detecting and countering threats to US or allied armed forces, and combating transnational criminal threats, including sanctions evasion'. Downright optimistic is he who can discern the specificity hereof. No wonder that *La Quadrature du Net* and Others, in their action of 25 October 2016 for annulment of the Commission's adequacy decision, build their 2nd plea in law on it, alleging that the 'six national security purposes […] cannot be considered as [an] objective criterion allowing a limitation to "purposes which are specific, strictly restricted and capable of justifying the interference"'.

Moreover, it remains an arduous task to assess these purposes *überhaupt* in the sense of 'restrictions', let alone that they would be convincing in light of the EU requirements in this field as operationalised in the CJEU's Data Retention judgment. Nevertheless, the Commission appears to see such considerations as nit-picking. In its adequacy decision, the Commission even attempts to embellish all of this[82] by *not* mentioning the six vague purposes by name, but by adducing their potential to detect and counter threats stemming from espionage, terrorism, weapons of mass destruction, threats to cyber-security, to the armed forces or military personnel, or in the context of transnational criminal threats to any of the other purposes. Such a misrepresentation is without honour. What we should be able to expect from the European Commission is that it protects the privacy of the European citizen and that it will inform the latter (via its communication and (draft) adequacy decision) in a clear and correct way, not that the Commission contemptuously approaches EU citizens with hollow and US-friendly rhetoric whilst continuing to give away their privacy via bulk-collection in order to facilitate almost any US-in-

[80] ibid, para 192 (emphasis added).

[81] Original letter annexed to the initial draft decision, p 4 para 3; Annex VI to the revised decision p 93 para 4.

[82] Commission Implementing Decision (revised decision) (n 64) para 74.

telligence purpose. As if all of this weren't enough already, the above mentioned *use* - 'limitations' will also be applicable to the *collection* of personal data that runs through trans-Atlantic submarine cables – located outside of US territory – and this – at least according to the Commission – is the icing on the cake in terms of reassurance.[83] Just for completion, for this specific type of data, collection is not liable for a request conformant to FISA-legislation or through a so-called *National Security Letter* of the FBI. Such a request - accentuated by the Commission - *will* be mandatory when the intelligence community wishes to retrieve information from companies *on* US territory that are 'self-certified' under the new Privacy Shield.[84]

This type of 'access' - and for that matter, a relief that for once this term is utilised in its proper, genuine meaning - would continuously need to be specific and limited, as it would require specific terms of selection or criteria. The fact that this would (even) be applicable to the PRISM-programme is considered a real windfall, at least by the Commission: this information is after all selected on the basis of individual selection criteria such as e-mail addresses and telephone numbers, and not through keywords or names of individuals.[85] As the Commission itself cannot resist emphasising, according to the *Civil Liberties Oversight Board* this would mean that in the US, when necessary, it would exclusively concern 'targeting specific [non-U.S.] persons about whom an individualised determination has been made'. Footnote 87 clarifies that the continuation of unleashing PRISM on US companies under the Privacy Shield will therefore *not* entail the undirected (unspecific) collection of data on a large scale. As you like it. PRISM apparently is *not* a programme for the collection of data on a large scale, or it is (at least) sufficiently selective to pass the test of European privacy law. It seems the Commission itself was mistaken when, at the end of November 2013, it claimed in its Safe Harbour communication that 'the large scale character of these programmes [...] [could] have as a consequence that, of all the data that was transferred in the framework of the safe harbour, more than was strictly necessary for, or proportionate to, the protection of national security, was consulted and further processed by the American authorities, as was determined by the exception foreseen in the Safe Harbour decision.' Moreover, as the Commission is so eager to allege, there is *empirical evidence* that the number of *targets* affected through PRISM on a yearly basis is 'relatively small *compared to the overall flow of data on*

[83] ibid, para 75.

[84] ibid, para 78.

[85] ibid, para 81 (sic).

the internet'.[86] The source for this statement is the 2014 annual report of the ODSI itself, hence it indeed appears that the PRISM-authorisation under FISA was applicable 'only' to 93.000 targets. Thus, nothing too large-scale for the Commission. Add to this the ODSI-warranty (in annex VI to the adequacy decision) that the bulk-collection only takes place on a 'small proportion of the internet', this including the capturing of data on the trans-Atlantic cables[87], and finally, everyone is convinced. Finally, what is added are a number of nugatory *additional* guarantees in the following paragraphs[88] such as, for instance, that it is insufficient that sigint was collected over the course of the 'routine activities of a foreign person' to spread it or to retain it permanently without there being other intelligence-based reasons for this.[89] EU citizens may rest assured: electronic communication regarding their day-to-day routines will not be retained permanently when there are no well-founded reasons to do so. All of this leads the Commission to conclude[90] that, in the US, there are ample rules in place specifically designed to ensure that 'any interference for purposes of national security with the fundamental rights of the persons whose personal data are transferred [...] under the EU-US Privacy Shield [is limited] to what is *strictly necessary* to achieve the legitimate objective in question' [emphasis added]. And with this alone the European citizen will have to make do. Those who thought that, following the *Schrems* judgment, there would be a real *issue* with the commercial transfers of personal data to the US simply because the companies on its territory had to run this data through the PRISM-filter were sorely mistaken. The CJEU based the invalidity of the Safe Harbour decision of the Commission on the techno-legal establishment that the latter had omitted to include in its decision that 'it must find, duly stating reasons, that the third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order, a level that is apparent in particular from the preceding paragraphs of the present judgment'.[91] In essence, the CJEU herewith refers to the substantive criteria of the Data Retention judgment. The European Commission's failure to mention 'that the United States in fact 'ensures' an adequate level of protection by reason of its domestic law or its international

[86] ibid, para 82.

[87] ibid.

[88] ibid, para 83-87.

[89] ibid, para 87.

[90] ibid, para 88.

[91] ibid, para 96.

commitments'[92] was enough for the Court to decide on a techno-legal breakpoint, 'without there being any need to examine the content of the safe harbour principles'.[93] Unfortunately, this (and only this) seems to be precisely what the European Commission remembers from the *Schrems* judgment, and is the (sole) reason why the Commission seems convinced that its reasoned ascertainment of the adequate safeguards in the US' privacy regime will suffice. While the *reasoning* aspect of this ascertainment is not open to question, the adequacy hereof is very equivocal - yet this was surely one of the *Schrems* judgment's demands. In brief, the presented argumentation is selective, often misleading, sometimes plain bogus. And last but not least, any effort to introduce a profound scrutiny based on the criteria established in the Data Retention judgment was omitted by the Commission, contrary to the CJEU *Schrems* judgment that specifically referred hereto.

5. DATA COLLECTION FOR LAW ENFORCEMENT OR PUBLIC INTEREST PURPOSES

In its adequacy decision, the Commission also evaluates the data protection-relevant limitations and safeguards afforded by US law within the *law enforcement* sphere. At the risk of sounding redundant, very much like all of the foregoing, the Commission's conclusion, un-surprisingly, is that the US data protection level is to be considered adequate.[94] Search and seizure by law enforcement authorities principally requires, according to the 4th amendment, a prior court order based on *'probable cause'*. In certain circumstances, however, the 4th amendment is not applicable because for some forms of electronic communication there are no legitimate privacy expectations. In such an event, a court order is not mandatory, and law enforcement may revert to a 'reasonability test'. The latter simply implies that a consideration is made between the level of infringement of an investigative measure with respect to an individual's privacy and the extent to which that measure is deemed necessary in function of legitimate government purposes like law enforcement (or another public interest). For the European Commission, this suffices to conclude that this *'captures the idea'* of necessity and proportionality under EU law.[95] The cold fact that the 4th amendment is quite simply not applicable to non-US citizens outside of US territory does not change the Commission's

[92] ibid, para 97.

[93] ibid, para 98.

[94] ibid, para 125.

[95] ibid, para 126.

viewpoint. The reasoning is that EU citizens would receive and enjoy the indirect protection that US companies - where their data is being stored - enjoy. The establishment that such a protection can be bypassed fairly easily via a simple reasonability test, and that the privacy of a company is not automatically at stake when law enforcement is after the private data of a user (only), is conveniently not addressed. According to the Commission, there are furthermore additional protective mechanisms, such as directives of the ministry of justice that allow law enforcement access to private data only on grounds that are labelled by the Commission as 'equivalent' to the necessity and proportionality requirement: these directives after all stipulate that the FBI must take recourse to the *least intrusive measure*.[96] That such a principle only addresses the *subsidiarity* of applying certain investigative measures, instead of dealing with their *necessity* or *proportionality* will probably be considered as nit-picking again. Finally, the Commission deals with the practice of administrative subpoenas (as issued at the time against the SWIFT US-hub). These are, as can be read, allowed only in particular circumstances and are subject to an independent judicial appraisal. What remains underemphasized - perhaps not to spoil the fun - is that the latter is only a possibility when a company refuses to spontaneously give effect to an administrative subpoena, thus forcing the government to have recourse to a judge for effecting said subpoena.

Likewise, when administrative subpoenas are issued in the *public interest*, similar limitations[97] are applicable. After all, administrations are only allowed to order access to data that is deemed relevant for matters under their competence - who would have thought any different? - and of course need to pass through the aforementioned reasonability test. All the more reason for the Commission, without wasting any more words on the matter, to promptly come to a conclusion[98] similar to the one on the collection of data in view of national security. As it is seemingly evidently stated, the US has rules in place that are specifically designed so that 'any interference for law enforcement or other public interest purposes with the fundamental rights of the persons whose personal data are transferred [will be limited] to what is *strictly necessary* to achieve the legitimate purpose in question' and that ensure 'effective legal protection against such interference'.

---

[96] ibid, para 127.

[97] ibid, para 129.

[98] ibid, para 135 (emphasis added).

The failure to safeguard against indiscriminate access to electronic communications by US law enforcement authorities has also been picked up by Digital Rights Ireland in its action of 16 September 2016 for annulment of the Privacy Shield adequacy decision. Its 8th plea in law alleges that, based on this very argument, the decision is invalid as a breach of the rights of privacy, data protection, freedom of expression and freedom of assembly and association, as provided for under the Charter and by the general principles of EU Law.

6. **CONCLUSION**

The Privacy Shield is all the added value of a scrap of paper – insufficient, lacking credibility, misleading – and nothing but a new jackstraw for the previous *Safe Harbour* approach. None of the US harbours have become safer, PRISM and the likes remain on track. The Commission has nevertheless gone through great lengths to set forth why all of us *should* believe that the 'limitations' and 'safeguards' available under US law are in line with the EU requirements of strict necessity and proportionality. The 2015 *Schrems* judgment, apparently, hasn't changed anything.

Luckily, it seems a matter of time only before the CJEU, in line with the latter decision, building on its 2014 Data Retention and 2016 *Tele2 Sverige AB* judgments, and following the actions for annulment brought in the fall 2016 by *Digital Rights Ireland* respectively *La Quadrature du Net* and Others, reinforced by the Irish High Court's recent judgment in *Data Protection Commissioner v Facebook Ireland Ltd. and Maximillian Schrems*, invalidates the Privacy Shield and annuls the Commission's corresponding adequacy decision.

In doing so, it will show that EU data protection standards are not up for grabs, neither in the trans-Atlantic relations nor in the EU's future relations with key trading partners in East and South-East Asia and with countries in Latin America and the European neighbourhood, which the Commission will negotiate or is negotiating similar 'shields' with,[99] like Japan.[100]

Likewise, the EU and data protection authorities, intelligence and law enforcement oversight bodies and courts throughout the EU should draw lessons on the internal level. They must in particular see to it that, irrespective of later access or use restrictions, preventative data retention or collection

[99] Commission (EC), 'Exchanging and Protecting Personal Data in a Globalised World' (Communication) COM(2017) 7 final, 10 January 2017.

[100] Commission (EC), 'Joint statement by Commissioner Věra Jourová and Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan on the state of play of the dialogue on data protection' (Joint Statement), 4 July 2017.

for protecting internal security or crime fighting is sufficiently selective, not only with respect to the categories of data to be retained, the means of communication affected and the retention period adopted, but also with respect to the persons concerned and the public affected.

7. SELECTED LITERATURE

Bennet CJ and Raab CD, 'The Adequacy of Privacy: the European Union Data Protection Directive and the North American Response' (1997) 13 The Information Society 245

Connorton PM, 'Tracking Terrorist Financing through SWIFT: When U.S. subpoenas and foreign privacy law collide' (2007) 76(1) Fordham L Rev 283

Coudert F, 'Schrems vs. Data Protection Commissioner: a slap on the wrist for the Commission and new powers for data protection authorities' (*European Law Blog* 2015) <https://lirias.kuleuven.be/bitstream/123456789/511500/1/FannyCoudert_Post+CJEU+Schrems_final.pdf>

Crowther H, 'Invalidity of the US Safe Harbor framework: what does it mean?' (2016) 11(2) JIPLP 88

Day R, 'Let the magistrates revolt: A review of search warrant applications for electronic in-formation possessed by online services' (2015) 64(2) U Kan L Rev 491

Darcy S, 'Battling for the Rights to Privacy and Data Protection in the Irish Courts' (2015) 31(80) Utrecht J of Intl and Eur L 131

De Busser E, *Data Protection in EU and US Criminal Cooperation* (Maklu 2009)

De Busser E, 'Purpose limitation in EU-US data exchange in criminal matters: the remains of the day' in Cools M and others (eds), *Readings on criminal justice, criminal law and policing* (vol 2, Maklu 2009)

De Busser E and Vermeulen G, 'Towards a coherent EU policy on outgoing data transfers for use in criminal matters? The adequacy requirement and the framework decision on data protection in criminal matters. A transatlantic exercise in adequacy' in Cools M and others (eds), *EU and International Crime Control* (vol 4, Maklu 2010)

De Busser E, 'Privatization of Information and the Data Protection Reform' in Gutwirth S and others (eds), *Reloading Data Protection* (Springer 2014)

De Hert P and De Schutter B, 'International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and Swift' in Martenczuk B and Van Thiel S (eds), *Justice, Liberty, Security: New Challenges for EU External Relations* (I.E.S. series nr. 11, VUB Press 2008)

Farrell H and Newman A, 'Transatlantic Data War. Europe fights back against the NSA' (2016) 95(1) Foreign Affairs 124

Flint D, 'Computers and internet: Sunk without a trace – the demise of safe harbor' (2015) 36(6) JBL 236

Gonzalez Fuster G, De Hert P and Gutwirth S, 'SWIFT and the vulnerability of transatlantic data transfers' (2008) 22(1-2) Intl Rev of L Computers & Technology 191

Greenwald G, 'NSA collecting phone records of millions of Verizon customers daily' *The Guardian* (London, 6 June 2013) <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>

Hildebrandt M, 'The rule of law in cyberspace?' (Inaugural Lecture at Radboud University Nijmegen, 2013) <http://works.bepress.com/mireille_ hildebrandt/48/>

Hustinx P, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' (2015) <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf>

Jaeger PT, Bertot JC and McClure CR, 'The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act' (2003) 20 Government Information Quarterly 295

Kirchner A, 'Reflections on privacy in the age of global electronic data processing with a focus on data processing practices of facebook' (2012) 6(1) Masaryk University Journal of Law and Technology 73

Koops BJ, 'The trouble with European data protection law' (2014) Tilburg Law School Legal Studies Research Paper Series 04/2015 <http://m.isaca.org/Groups/Professional-English/privacy-data-protection/GroupDocuments/2014-08-24%20%20The%20Trouble%20with%20European%20Data%20Protection%20 Law.pdf>

Long WJ and Quek MP, 'Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise' (2002) 9(3) JEPP 325

MacAskill E and others, 'GCHQ taps fibre-optic cables for secret access to world's communications' *The Guardian*, (London, 21 June 2013) <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications -nsa>

Ni Loideain N, 'The End of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law' (2016) 19(8) J Internet L 7

Papandrea MR, 'Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment' (2014) 94(2) Boston U L Rev 449

Peers S, 'The exchange of personal data between Europol and the USA' (2003) Statewatch Analysis no 15 <www.statewatch.org>

Piodi F and Mombelli I, 'The ECHELON Affair. The European Parlia-ment and the Global Interception System 1998 – 2002' (2014) European Parliament History Series <http://www.europarl.europa.eu/EPRS/EPRS_STUDY_538877_AffaireEchelon-EN.pdf>.

Reding V, 'The European data protection framework for the twenty-first century' (2012) 2(3) International Data Privacy Law 119

Simmons N, 'Facebook and the Privacy Frontier' (2012) 33(3) JBL 58

Vermeulen G, 'Transatlantisch monsterverbond of verstandshuwelijk? Over het verschil tussen oorlog en juridische strijd tegen terreur en de versterkte politie- en justitiesamenwerking tussen EU en VS' (2004) 25(1) Panopticon 90

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 Svantesson DJB & Kloza D (eds), *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy, European Integration and Democracy Series* (vol 4, Intersentia 2017)

X, 'Taking a bite at the Apple. The FBI's legal battle with the maker of iPhones is an escalation of a long-simmering conflict about encryption and security' *The Economist* (London, 27 February 2016) <http://www.economist.com/news/science-and-technology/21693564-fbis-legal-battle-maker-iphones-escalation>

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