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

Gert Vermeulen

Full Professor 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
Extraordinary Professor of Evidence Law, Faculty of Law, Maastricht University
Privacy Commissioner, Belgian DPA

Forthcoming in:

Svantesson, Dan J.B. and Dariusz Kloza (eds.) (2016) Transatlantic Data Privacy Relationships as a Challenge for Democracy; European Integration and Democracy Series, Vol. 4, Intersentia, Cambridge

---

1. Background: Inadequacy of the US data protection regime: clear to everyone after *Snowden*

Already the Europol-US agreement of December 20, 2002[1] and the EU-US mutual assistance treaty in criminal matters of June 25, 2003[2], both concluded in the immediate aftermath of 9/11, set the tone. 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[3] required so. Purpose limitation (specialty)[4] in the use of data provided by Europol or EU member states proved an almost nugatory concept, where the US were allowed to freely share information that was procured in criminal cases for purely administrative or intelligence purposes.[5] 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.[6] Moreover, SWIFT itself defected herein, as its US hub did not endorse the so-called *Safe Harbour* principles.[7] These had been developed in 2000 by the European

---

[1] Supplemental agreement between the Europol Police Office and the United States of America on the exchange of personal data and related information, 20.12.2002. Available via: https://www.europol.europa.eu/content/supplemental-agreement-between-europol-police-office-and-united-states-america.

[2] Agreement on mutual legal assistance between the European Union and the United States of America, OJ L 181/34, 19.07.2003. Available via: http://ec.europa.eu/world/agreements/downloadFile.do?fullText=yes&treatyTransId=10101.

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995. Available via: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[4] E. De Busser (2009). Purpose limitation in EU-US data exchange in criminal matters: the remains of the day. In: M. Cools, S. De Kimpe, B. De Ruyver, M. Easton, L. Pauwels, P. Ponsaers, G. Vande Walle, et al. (Eds.). Readings on criminal justice, criminal law and policing, (Vol. 2). Antwerp, Belgium ; Apeldoorn, The Netherlands: Maklu, pp. 163–201.

[5] S. Peers (2003). The exchange of personal data between Europol and the USA. Statewatch Analysis, pp. 1-3. Available via: www.statewatch.org; G. Vermeulen (2004). Transatlantisch monsterverbond of verstandshuwelijk? Over het verschil tussen oorlog en juridische strijd tegen terreur en de versterkte politie- en justitiesamenwerking tussen EU en VS. *Panopticon*, 25(1), pp. 90-107; P. De Hert & B. De Schutter (2008). International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and Swift. In: B. MARTENCZUK and S. VAN THIEL (eds.), Justice, Liberty, Security: New Challenges for EU External Relations, VUB Press, Brussels, (I.E.S. series nr. 11), pp. 326-327 and pp. 329-333.

[6] See the Privacy Commission's opinion on the Transfer of Personal Data by the CSLR SWIFT by Virtue of UST (OFAC), 37/2006. Available via: https://www.privacycommission.be/sites/privacycommission/files/documents/advies_37_2006_1.pdf; Furthermore, see: P.M. Connorton (2007). Tracking Terrorist Financing through SWIFT: When U.S. subpoenas and foreign privacy law collide. *Fordam Law Review*, 76(1), pp. 283-322.

[7] G. Gonzalez Fuster, P. De Hert & S. Gutwirth (2008). SWIFT and the vulnerability of transatlantic data transfers. *International Review of Law Computers & Technology*, Vol. 22,Nos. 1-2, March –July, pp. 191-202.

Commission[8] to ensure that, given that the US data protection regime in itself could not be qualified as adequate, commercial EU-US data transfers would nonetheless be enabled.[9] Companies that indicated (and self-certified) to comply 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 all but 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 filtering capacity proper) to obtain *bulk*-access on a case-by-case basis to these intra-European payment transactions. This TFTP-agreement (*Terrorist Financing Tracking Program*[10]), completed in 2010, furthermore contains an article in which the US Treasury is axiomatically declared as adequate in terms of data protection.[11] Notwithstanding, 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 reasonable doubt. That the Foreign Intelligence Surveillance Act (FISA)[12], altered post-9/11 with the Patriot Act[13] and further expanded in 2008[14], allowed the US to monitor – both with or without a court order – electronic communication in a way that was disproportionate, worldwide and in bulk, was clear as well.[15] This and more was confirmed in the Summer of 2013 with the revelations of whistleblower *Edward Snowden.*[16] These revelations were particularly shocking because of the revealed extent of the interception practices of the NSA (National Security

[8] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, 2000/520/EC, OJ L 215, 25.08.2000.

[9] See, f.i.: W.J. Long & M.P. Quek (2002). Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise. *Journal of European Public Policy*, 9(3), pp. 325-344.

[10]Agreement between the European Union and the United States of America 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, OJ L 008, 13.01.2010. Available via: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:22010A0113%2801%29&from=EN.

[11] Article 6 of the TFTP Agreement (fn. 6) 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."

[12] The Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801-11, 1821-29, 1841-46, 1861-62, 1871. Available via: https://www.law.cornell.edu/uscode/text/50/chapter-36/subchapter-I.

[13] Uniting and Strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) Act of 2001, Pub. L. 107-56; 10/26/01. Available via: https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf.; See also: P.T. Jaeger, J.C. Bertot & C.R. McClure (2003). The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act. *Government Information Quarterly*, no. 20, pp. 295-314.

[14]Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L.110-261; 7/10/2008. Available via: https://www.gpo.gov/fdsys/pkg/PLAW-110publ261/pdf/PLAW-110publ261.pdf.

[15] E. De Busser (2009). Purpose limitation in EU-US data exchange in criminal matters: the remains of the day. In: M. Cools, S. De Kimpe, B. De Ruyver, M. Easton, L. Pauwels, P. Ponsaers, G. Vande Walle, et al. (Eds.). Readings on criminal justice, criminal law and policing, (Vol. 2). Antwerp, Belgium ; Apeldoorn, The Netherlands: Maklu, pp. 163–201; E. De Busser (2009). Data Protection in EU and US Criminal Cooperation, Antwerp–Apeldoorn–Portland: Maklu, 474p.

[16] 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: G. Greenwald (2013). NSA collecting phone records of millions of Verizon customers daily. *The Guardian*, 06.06.2013. Available via: http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; See also: M-R. Papandrea (2014). Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment. *Boston University Law Review*, 94(2), pp. 449-544.

Agency) – *inter alia* through the PRISM programme – and the British intelligence service GCHQ's (Government Communications Headquarters)[17] – which for years had spied on *Belgacom International Carrier Service* (Bics). As a subsidiary of the current *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, this regardless of the fact that many were aware that these five, within the context of Echelon, were already monitoring worldwide satellite communications for decennia, including for commercial purposes. Already in 2000, the European Parliament had instigated an investigative commission against these practices.[18] From the US side, the publication of NSA-newsletters in the Summer of 2015 as a result of the *Snowden* revelations, plainly confirmed these allegations.[19]

2. Safe Harbour unsafe

Using the leverage handed to her with the Lisbon Treaty[20], former Commissioner of Justice *Reding* launched an ambitious legislative data protection package at the outset of 2012.[21] A proposed Regulation was initiated to replace Directive 95/46[22] , 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.[23] In December 2015, after a great deal of to-ing and fro-ing – and almost four years and a European Commission later – political agreement was reached on the new Regulation and the Directive.[24] Both of them will be formally accepted by the Summer and member states are due to apply them within as little as two years' time. The adequacy requirement for data transfers to third states

[17] The involvement of the British GCHQ was revealed by *the Guardian* on the 21st of June, 2013. See: E. MacAskill, J. Borger, N. Hopkins, N. Davies & J. Ball (2013). GCHQ taps fibre-optic cables for secret access to world's communications. *The Guardian*, 21.06.2013. Available via: http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

[18] See European Parliament decision setting up a temporary committee on the ECHELON interception system (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: 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, 11.07.2001. See also: F. Piodi & I. Mombelli (2014). The ECHELON Affair. The European Parliament and the Global Inter-ception System 1998 – 2002, European Parliament History Series, European Parliamentary Research Service (EPRS), Luxembourg. Available via: http://www.europarl.europa.eu/EPRS/EPRS_STUDY_538877_AffaireEchelon-EN.pdf.

[19] See, f.i.: H. Farrell & A. Newman (2016). Transatlantic Data War. Europe fights back against the NSA. *Foreign Affairs*, 95(1), pp. 124-133.

[20] Treaty of Lisbon Amending the Treaty on European Union and the Treaty establishing the European Community, OJ 2007/C 306/01, 17.12.2007.

[21] V. Reding (2012). The European data protection framework for the twenty-first century. *International Data Privacy Law*, Vol. 2, No. 3, pp. 119-129; Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: 'Safeguarding Privacy in a Connected World -A European Data Protection Framework for the 21st Century, COM (2012) 9 final.

[22] C.J. Bennet & C.D. Raab (1997). The Adequacy of Privacy: the European Union Data Protection Directive and the North American Response. The Information Society, Vol. 13, p. 252.

[23] 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, OJ L 350, 30.12.2008; See also: E. De Busser & G. Vermeulen (2010). 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: M. Cools, B. De Ruyver, M. Easton, L. Pauwels, P. Ponsaers, G. Vande Walle, T. Vander Beken, et al. (Eds.). EU and International Crime Control (Vol. 4). Antwerpen–Apeldoorn–Portland: Maklu, pp. 95–122.

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

moreover remains intact. *Reding* also took up the defense for EU citizens for what concerns US access to their personal data.[25] Just 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)[26] 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)[27] (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'[28], 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 national security'* [emphasis added]. 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 (annex I, paragraph 4). 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' [emphasis added].[29]

3. Safe Harbour is dead

Real urgency in the negotiations with the US only (re)surfaced following the ruling of the Court of Justice on October 6, 2015 in response to the appeal of *Max Schrems* against the Irish privacy commissioner (in proceedings against *Facebook*[30], that has its European headquarters established in Dublin) before the Irish High Court.[31] The latter had requested a preliminary ruling herein of the Court in Luxembourg, and namely 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 held a contradictory argumentation based on the post-*Snowden* ascertainment that *Facebook* was active in the PRISM-programme, regardless of its self-certification under the Safe Harbour principles).[32] The Court concluded

[25]See, f.i.: E. De Busser (2014). Privatization of Information and the Data Protection Reform. In: S. Gutwirth et al. (eds.). Reloading Data Protection. Springer Science+ Business Media Dordrecht, pp. 129-149.

[26] European Commission (2013). Communication from the Commission to the European Parliament and the Council. Rebuilding Trust in EU-US Data Flows, COM(2013) 846 final. Available via: http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf.

[27] European Commission (2013). Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM(2013) 847 final. Available via: http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf.

[28] Report on the Findings of the EU Co-Chairs of the Ad Hoc EU-US Working Group on Data Protection, 27.11.2013. Available via: http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf.

[29] Safe Harbour Communication (fn. 22), point 7.1.

[30]See, f.i.: N. Simmons (2012). Facebook and the Privacy Frontier. *Business Law Review*, 33(3), pp. 58-62. Available via: http://www.kluwerlawonline.com/document.php?id=BULA2012013.

[31] CJEU October 6, 2015, case C-362/14 (Maximillian Schrems v. Data Protection Commissioner).

[32] A. Kirchner (2012). Reflections on privacy in the age of global electronic data processing with a focus on data processing practices of facebook. Masaryk University Journal of Law and Technology, 6(1), pp. 73-86; M. Hildebrandt (2013). The rule of

inter alia that '[t]he right to respect for 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*' [emphasis added] (paragraph 34). The Court furthermore recalled, with explicit reference to its Data Retention judgement of April 8, 2014[33] (in which the Court had declared the Data Retention Directive invalid) and its previous judgements as cited under points 54 & 55 of its Data Retention judgement, 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 […]' [emphasis added] (paragraph 91). Still with reference to the Data Retention judgement (and the cited case-law under point 52 hereof), the Court 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*' [emphasis added] (paragraph 92), whereby of course a '[l]egislation *is not limited to what is strictly necessary* where it authorises, on a generalised basis, *storage* of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in 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' [emphasis added] (paragraph 93). 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 omitted to implement such an assessment in its Safe Harbour decision, the Court decided on the invalidity of the latter. Hence, with the *Schrems* case, the Court 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 as 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

law in cyberspace?, Inaugural Lecture, Chair of Smart Environ-ments, Data Protection and the Rule of Law, Institute of Computing and Information Sciences (iCIS), Nijmegen: Radboud University. Available via: http://works.bepress.com/mireille_hildebrandt/48/; B.J. Koops (2014). The trouble with European data protection law. *International Data Privacy Law*, doi:10.1093/idpl/ipu023. Available via: http://m.isaca.org/Groups/Professional-English/privacy-data-protection/GroupDocuments/2014-08-24%20%20The%20Trouble%20with%20European%20Data%20Protection%20Law.pdf.; F. Coudert (2015). Schrems vs. Data Protection Commissioner: a slap on the wrist for the Commission and new powers for data protection authorities, European Law Blog, 15.10.2015. Available online via: https://lirias.kuleuven.be/bitstream/123456789/511500/1/FannyCoudert_Post+CJEU+Schrems_final.pdf.; R. Day (2015). Let the magistrates revolt: A review of search warrant applications for electronic in-formation possessed by online services, *University of Kansas Law Review*, 64(2), pp. 491-526; S. Darcy (2015). Battling for the Rights to Privacy and Data Protection in the Irish Courts. *Utrecht Journal of International and European Law*, 31(80), pp.131–136. DOI: http://doi.org/10.5334/ujiel.cv; D. Flint (2015). Computers and internet: Sunk without a trace – the demise of safe harbor. Business Law Review, 36(6), pp. 236-237. Available via: http://www.kluwerlawonline.com/document.php?id=BULA2015031; H. Crowther (2016). Invalidity of the US Safe Harbor framework: what does it mean? *Journal of Intellectual Property Law & Practice*, 11(2), pp. 88-90; N. Ni Loideain (2016). The End of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law, *Journal of Internet Law*, Vol. 19, No. 8, February 2016.

[33] CJEU April 8, 2014, cases C 293/12 & C 594/12, ECLI:EU:C:2014:238 (Digital Rights Ireland a.o.).

emotions. In a communication on the very day of the Court'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, since its Safe Harbour communication, the Commission was working with the US authorities 'to make data transfers *safer* for European citizens' [emphasis added] and that, in light of the *Schrems* judgement, it would continue to work 'towards a renewed and *safe* framework for the transfer of personal data across the Atlantic' [emphasis added].[34]

4. Long live the privacy shield!

On February 29, 2016, the Commission presented its eagerly awaited 'solution'. It launched a new communication, titled 'Transatlantic Data Flows: Restoring Trust through Strong Safeguards'[35], and immediately attached hereto – in replacement of the invalidated Safe Harbour decision – its draft adequacy decision[36] 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 U.S. public authorities on national security grounds'. Before we can evaluate 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. Completing 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 now presented by the privacy shield – the Safe Harbour regime did not foresee any of these – are convincing enough. The convulsive way in which the European Commission tried to convince everyone, through the means of its communication and the attached draft adequacy decision, of the satisfactory nature of this new regime, and that from now on 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. As it turns out, negotiating (too) tough was apparently not considered an option herein. 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 scarce counter-examples like the Apple-

[34] Communication from the Commission to the European Parliament and the Council 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), COM(2015) 566 final, 06.11.2015.

[35] Communication from the Commission to the European Parliament and the Council. Transatlantic Data Flows: Restoring Trust through Strong Safeguards, COM(2016) 117 final, Brussels, 29 February 2016.

[36] 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.

FBI clash[37] aside. In the meantime, the very minimum is to burst the bubble of the European Commission's discourse in the privacy shield communication and ditto 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 show this.

5. Limitations and safeguards regarding data collection in the interest of national security

a. Collection and access v. access and use: One big amalgamation

The Commission 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' (see paragraph 55 of the draft adequacy decision) for the purpose of national security, public interest or law enforcement, will be sufficient in light of EU law to allude 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' hereof. 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 the leg of its reader. To the extent still necessary, it suffices to recall the previously mentioned Data Retention judgement of the Court of Justice. 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 mirage 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 casu* the US intelligence or law enforcement services) is bound by strict requirements. After all, one of the reasons why the Court dismissed the Data Retention directive as invalid (see paragraph 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.
Apart from this, the Court hackled 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' (paragraph 60). 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*

[37] See, f.i.: The economist (2016). 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, 27.02.2016. Available online via: http://www.economist.com/news/science-and-technology/21693564-fbis-legal-battle-maker-iphones-escalation.

restricted to the purpose of preventing and detecting *precisely defined* serious offences or of conducting 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' [emphasis added] (paragraph 61). 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' [emphasis added] (paragraph 62). *Mutatus mutandis* (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) both the necessity and proportionality requirements can be firmly derived from the Data Retention judgement, 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 'limitations' of US processing of and interference with EU personal data as presented by the US. This, even more so because of the prior operationalisation hereof by the Court's Data Retention judgement. Unfortunately, we are presented with the manifest absence hereof. From a substantive perspective, it is moreover the case that the guarantees in terms of 'collection' are clearly insufficient, since e.g. bulk collection of data remains perfectly possible under certain scenario's. Not only - and contrary to how it is presented by the Commission - will the privacy shield fail to solve this with the limitations it contains in terms of 'access and use', the latter's limitations are inherently flawed as well, as they do not comply with nor mirror the (EU) requirements of strict necessity and proportionality.

b. Bulk collection remains possible

In itself it is gratifying (paragraph 58 of the draft adequacy decision) that under PPD-28 (the *Presidential Policy Directive* 28 of January 17, 2014)[38] intelligence operations in the plane of sigint (*Signals Intelligence,* or the interception of electronic communication) will from now on only be allowed for purposes of foreign or contra-*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. Whoopty doo.

As far as diversions go, this is a big one. Following the *Schrems* judgement, this is evidently no longer the stake. The real question is whether the limitations to 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, and this 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' (paragraph 58), and members of the intelligence community [emphasis added] '*should* require that, *wherever practicable*, collection

[38] Presidential Policy Directive -- Signals Intelligence Activities. Presidential policy directive/PPD-28, 17.01.2014. Available via: https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

should be focused on specific foreign intelligence targets or topics *through the use of discriminants* (e.g. specific facilities, selection terms and identifiers' (paragraph 59). 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' does evidently 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 'specific' circumstances (that are not very 'specific' to begin with, like 'the identification of new or emerging threats') will still take place. The Commission from 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 31) that the feasibility report, which was supposed to be presented to president Obama by the Director of National Intelligence with reference to the possibility to develop 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 rallies behind the ODNI's own estimation that bulk collection will not be the rule (rather than the exception) - 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 (paragraph 60). Now that would have been a proper good deal wrong. In addition, the Commission sees an extra 'safeguard' in the fact that the potential 'discriminants' shall be determined by high ranking policy makers, and that they will be (re)evaluated on a regular basis (paragraph 60). 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 (infra, under section 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 (paragraph 63): bulk-collection needs to stay 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, and with this, collection is by no means compliant with the tight restrictions of EU privacy law in terms of data collection.

c. Access and use do not comply with strict necessity and proportionality requirements

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 (page 4, third indent of annex VI to the draft adequacy decision): '*detecting and countering certain activities of foreign powers, counterterrorism, counter-proliferation, cybersecurity, detecting and countering threats to U.S. or allied armed forces, and combating transnational criminal threats, including sanctions evasion*'. Downright voluntaristic is he who can discern the specificity hereof. 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 Court's Data Retention judgement. Nevertheless, the Commission appears to classify such considerations as nitpicking. In its draft adequacy decision, the Commission even attempts to embellish all of this (paragraph 61) by *not* mentioning the six vague purposes by name, but by adducing their potential to detect and tackle threats in the sphere of espionage, terrorism and weapons of mass destruction, against armed forces or military personnel, or in the context of transnational crime. 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-intelligence purpose. As if all of this weren't enough already, the above mentioned *use*-'limitations' will also be applicable for the *collection* of personal data that runs through trans-Atlantic submarine cables - and that as such are located outside of US territory - and this - at least according to the Commission - is the icing on the cake in terms of reassurance (paragraph 62). 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 (paragraph 65).
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 to be a real windfall, at least by the Commission: this information is after all selected on the basis of individual selection criteria like e.g. email addresses and telephone numbers, and not through keywords or names of individuals (sic, paragraph 68). As the Commission itself cannot resist but stress, 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 72 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. As 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 amount of *targets* affected through PRISM on a yearly basis is 'relatively small *compared to the overall flow of data on the internet'* (recital 69). 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-scaly for the Commission. Add to this the ODSI-warranty (in annex VI to the draft 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 (paragraph 69), and finally, everyone is convinced. Finally, what is added are a number of nugatory *additional* guarantees in the following paragraphs (70-74) like, 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 (recital 74). Hence, 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 (paragraph 74) that, in the US, there are ample rules in place specifically designed as to insure that 'any interference for purposes of national security with the fundamental rights of the persons whose data is transferred from the EU tot the US by means of the privacy shield, is limited to what is *strictly necessary* to realise that legitimate purpose' [emphasis added]. And with this alone the European citizen will have to make do. Those who thought that, following the *Schrems* judgement, 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 Court 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' (paragraph 96). In essence, the Court herewith refers to the substantive criteria of the Data Retention judgement. The

European Commission's non-mentioning 'that the United States in fact ‘ensures’ an adequate level of protection by reason of its domestic law or its international commitments' (paragraph 97) 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' (paragraph 98). Unfortunately, this (and only this) seems to be precisely what the European Commission remembers from the *Schrems* judgement, and 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 without question, the adequacy hereof is very equivocal - yet this was surely one of the *Schrems* judgement'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 as established in the Data Retention judgement was omitted by the Commission, contrarious to the Court's *Schrems* judgement that specifically referred hereto.

d. Ombudsperson

Elaborating on the ultimate 'safeguard' that was introduced via the creation of a privacy shield ombudsperson is largely irrelevant. The Commission’s draft adequacy decision emphasises the independence of the mechanism, devoid of any instruction from the US intelligence community (paragraph 104). This notwithstanding, it suffices to say that it revolves around a vice-secretary of US State Department, an instance not without its partiality (to put it mildly) in terms of national security. Moreover, there is absolutely no direct EU-involvement in the ombudsperson mechanism. Putting two and two together, it becomes apparent that the Commission's viewpoint is rather gratuitous. Be as it may, the only real engagement of the ombudsperson is to evaluate potential complaints and to confirm that US legislation, including the aforementioned 'limitations' (which are, by repetition, insufficient in light of EU law) have been observed, and should that not be the case (which in such an event shall *not* be informed towards to plaintiff, nor whether he or she was the subject of a surveillance measure) whether this situation is resolved (paragraph 104 and point 4.e of annex III to the draft adequacy decision). Last but not least, the curtain is pulled on potential complaints featuring - with good reason - arguments that the privacy shield in itself is not conformant with EU data protection requirements. The ODNI letter to this point (annex III to the draft adequacy decision, point 4.g) simply, and laconically, states that the Ombudsperson mechanism shall in any such case refrain from being applicable. In any interpretation, this renders the Ombudsperson nothing more than a subterfuge measure.

6. Limitations and safeguards regarding data collection in the interest of law enforcement or public interest

In its draft 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 above, the Commission's conclusion is non-surprisingly that the US data protection level is to be considered as adequate (paragraph 106). 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 (paragraph 107). 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 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 are after the private data of a user (only), is conveniently not addressed. According to the Commission, there are furthermore additional protective mechanisms, like for instance directives of the ministry of justice that allow law enforcement access to private data only based 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* (paragraph 108). 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 nitpicking 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 effectuating said subpoena.
Likewise, when administrative subpoenas are issued in the *public interest*, similar limitations (so we learn in paragraph 110) 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 (paragraph 111) 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 purposes of law enforcement or another public interest with the fundamental rights of persons whose data are transferred from the EU to the US under the privacy shield, will be limited to what is *strictly necessary* to realise that legitimate purpose' [emphasis added] and 'that guarantee an effective judicial protection against such interferences'.

7. Conclusion

The European Commission's draft adequacy decision is all the added value of a scrap of paper, nothing more: insufficient, lacking credibility, misleading. The Commission has nevertheless gone through the lengths to extensively 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 *Schrems* case, apparently, hasn't changed anything. The privacy shield is nothing but a new jackstraw for the previous *Safe Harbour* approach. As it is, we are simply presented with the same old thing in a new coat of paint, without any intrinsic change in the situation in the US. None of the US harbours have become safer, PRISM and the likes remain on track. But was anyone naïve enough to think differently? The only novel thing is that the European Commission has gone above and beyond to = a Trojan horse - that is all the privacy shield really is - and then push it in front of the EU's gates. Heed the EU citizen not to take it inside!

References

Kirchner (2012). Reflections on privacy in the age of global electronic data processing with a focus on data processing practices of facebook. *Masaryk University Journal of Law and Technology*, 6(1), pp. 73-86.

Agreement between the European Union and the United States of America 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, OJ L 008, 13.01.2010. Available via: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:22010A0113%2801%29&from=EN

Agreement on mutual legal assistance between the European Union and the United States of America, OJ L 181/34, 19.07.2003. Available via: http://ec.europa.eu/world/agreements/downloadFile.do?fullText=yes&treatyTransId=10101

B.J. Koops (2014). The trouble with European data protection law. *International Data Privacy Law*, doi:10.1093/idpl/ipu023. Available via: http://m.isaca.org/Groups/Professional-English/privacy-data-protection/GroupDocuments/2014-08-24%20%20The%20Trouble%20with%20European%20Data%20Protection%20Law.pdf.

C.J. Bennet & C.D. Raab (1997). The Adequacy of Privacy: the European Union Data Protection Directive and the North American Response. The Information Society, Vol. 13, p. 252.

CJEU April 8, 2014, cases C 293/12 & C 594/12, ECLI:EU:C:2014:238 (Digital Rights Ireland a.o.).

CJEU October 6, 2015, case C-362/14 (Maximillian Schrems v. Data Protection Commissioner).

Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, 2000/520/EC, OJ L 215, 25.08.2000.

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.

Communication from the Commission to the European Parliament and the Council 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), COM(2015) 566 final, 06.11.2015.

Communication from the Commission to the European Parliament and the Council. Transatlantic Data Flows: Restoring Trust through Strong Safeguards, COM(2016) 117 final, Brussels, 29 February 2016.

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, OJ L 350, 30.12.2008.

D. Flint (2015). Computers and internet: Sunk without a trace – the demise of safe harbor. *Business Law Review*, 36(6), pp. 236-237. Available via: http://www.kluwerlawonline.com/document.php?id=BULA2015031

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995. Available via: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

E. De Busser & G. Vermeulen (2010). 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: M. Cools, B. De Ruyver, M. Easton, L. Pauwels, P. Ponsaers, G. Vande Walle, T. Vander Beken, et al. (Eds.). EU and International Crime Control (Vol. 4). Antwerpen–Apeldoorn–Portland: Maklu, pp. 95–122.

E. De Busser (2009). Data Protection in EU and US Criminal Cooperation, Antwerp–Apeldoorn–Portland: Maklu, 474p.

E. De Busser (2009). Purpose limitation in EU-US data exchange in criminal matters: the remains of the day. In: M. Cools, S. De Kimpe, B. De Ruyver, M. Easton, L. Pauwels, P. Ponsaers, G. Vande Walle, et al. (Eds.). Readings on criminal justice, criminal law and policing, (Vol. 2). Antwerp, Belgium ; Apeldoorn, The Netherlands: Maklu, pp. 163–201

E. De Busser (2014). Privatization of Information and the Data Protection Reform. In: S. Gutwirth et al. (eds.). Reloading Data Protection. Springer Science+ Business Media Dordrecht, pp. 129-149.

E. MacAskill, J. Borger, N. Hopkins, N. Davies & J. Ball (2013). GCHQ taps fibre-optic cables for secret access to world's communications. *The Guardian*, 21.06.2013. Available via: http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

European Commission (2013). Communication from the Commission to the European Parliament and the Council. Rebuilding Trust in EU-US Data Flows, COM(2013) 846 final. Available via: http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf

European Commission (2013). Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM(2013) 847 final. Available via: http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf.

European Parliament decision setting up a temporary committee on the ECHELON interception system. Available via: http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=B5-2000-0593&language=EN.

F. Coudert (2015). Schrems vs. Data Protection Commissioner: a slap on the wrist for the Commission and new powers for data protection authorities, European Law Blog, 15.10.2015. Available online via: https://lirias.kuleuven.be/bitstream/123456789/511500/1/FannyCoudert_Post+CJEU+Schrems_final.pdf.

F. Piodi & I. Mombelli (2014). The ECHELON Affair. The European Parliament and the Global Interception System 1998 – 2002, European Parliament History Series, European Parliamentary Research Service (EPRS), Luxembourg. Available via: http://www.europarl.europa.eu/EPRS/EPRS_STUDY_538877_AffaireEchelon-EN.pdf.

Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L.110-261; 7/10/2008. Available via: https://www.gpo.gov/fdsys/pkg/PLAW-110publ261/pdf/PLAW-110publ261.pdf.

G. Gonzalez Fuster, P. De Hert & S. Gutwirth (2008). SWIFT and the vulnerability of transatlantic data transfers. *International Review of Law Computers & Technology*, Vol. 22,Nos. 1-2, March –July, pp. 191-202.

G. Greenwald (2013). NSA collecting phone records of millions of Verizon customers daily. *The Guardian*, 06.06.2013. Available via: http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

G. Vermeulen (2004). Transatlantisch monsterverbond of verstandshuwelijk? Over het verschil tussen oorlog en juridische strijd tegen terreur en de versterkte politie- en justitiesamenwerking tussen EU en VS. *Panopticon*, 25(1), pp. 90-107.

H. Crowther (2016). Invalidity of the US Safe Harbor framework: what does it mean? *Journal of Intellectual Property Law & Practice*, 11(2), pp. 88-90.

H. Farrell & A. Newman (2016). Transatlantic Data War. Europe fights back against the NSA. *Foreign Affairs*, 95(1), pp. 124-133.

M. Hildebrandt (2013). The rule of law in cyberspace?, Inaugural Lecture, Chair of Smart Environments, Data Protection and the Rule of Law, Institute of Computing and Information Sciences (iCIS), Nijmegen: Radboud University. Available via: http://works.bepress.com/mireille_hildebrandt/48/.

M-R. Papandrea (2014). Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment. *Boston University Law Review*, 94(2), pp. 449-544.

N. Ni Loideain (2016). The End of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law, *Journal of Internet Law*, Vol. 19, No. 8, February 2016.

N. Simmons (2012). Facebook and the Privacy Frontier. *Business Law Review*, 33(3), pp. 58-62. Available via: http://www.kluwerlawonline.com/document.php?id=BULA2012013.

P. De Hert & B. De Schutter (2008). International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and Swift. In: B. MARTENCZUK and S. VAN THIEL (eds.), Justice, Liberty, Security: New Challenges for EU External Relations, VUB Press, Brussels, (I.E.S. series nr. 11), pp. 326-327 and pp. 329-333.

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

P.M. Connorton (2007). Tracking Terrorist Financing through SWIFT: When U.S. subpoenas and foreign privacy law collide. *Fordam Law Review*, 76(1), pp. 283-322.

P.T. Jaeger, J.C. Bertot & C.R. McClure (2003). The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act. *Government Information Quarterly*, no. 20, pp. 295-314.

Presidential Policy Directive -- Signals Intelligence Activities. Presidential policy directive/PPD-28, 17.01.2014. Available via: https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities

Privacy Commission's opinion on the Transfer of Personal Data by the CSLR SWIFT by Virtue of UST (OFAC), 37/2006. Available via: https://www.privacycommission.be/sites/privacycommission/files/documents/advies_37_2006_1.pdf.

R. Day (2015). Let the magistrates revolt: A review of search warrant applications for electronic information possessed by online services, *University of Kansas Law Review*, 64(2), pp. 491-526.

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, 11.07.2001.

Report on the Findings of the EU Co-Chairs of the Ad Hoc EU-US Working Group on Data Protection, 27.11.2013. Available via: http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf.

S. Darcy (2015). Battling for the Rights to Privacy and Data Protection in the Irish Courts. *Utrecht Journal of International and European Law*, 31(80), pp.131–136. DOI: http://doi.org/10.5334/ujiel.cv

S. Peers (2003). The exchange of personal data between Europol and the USA. Statewatch Analysis, pp. 1-3. Available via: www.statewatch.org.

Supplemental agreement between the Europol Police Office and the United States of America on the exchange of personal data and related information, 20.12.2002. Available via: https://www.europol.europa.eu/content/supplemental-agreement-between-europol-police-office-and-united-states-america.

The economist (2016). 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, 27.02.2016. Available online via: http://www.economist.com/news/science-and-technology/21693564-fbis-legal-battle-maker-iphones-escalation.

The Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801-11, 1821-29, 1841-46, 1861-62, 1871. Available via: https://www.law.cornell.edu/uscode/text/50/chapter-36/subchapter-I.

Treaty of Lisbon Amending the Treaty on European Union and the Treaty establishing the European Community, OJ 2007/C 306/01, 17.12.2007.

Uniting and Strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) Act of 2001, Pub. L. 107-56; 10/26/01. Available via: https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf.

V. Reding (2012). The European data protection framework for the twenty-first century. *International Data Privacy Law*, Vol. 2, No. 3, pp. 119-129; Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: 'Safeguarding Privacy in a Connected World -A European Data Protection Framework for the 21st Century, COM (2012) 9 final.

W.J. Long & M.P. Quek (2002). Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise. *Journal of European Public Policy*, 9(3), pp. 325-344.