Issue | July 2015
No.2 | Special Issue: Privacy

Montesquieu Law Review

The war on terror and the protection of personal data

Philippe Ch.-A Guillot, Professor of International Relations, French Air Force Academy

Program supported by the ANR
n°ANR-10-IDEX-03-02

Forum Montesquieu
Faculté de droit et science politique
université de BORDEAUX

The war on terror and the protection of personal data

Philippe Ch.-A Guillot, Professor of International Relations, French Air Force Academy

Suggested citation: Philippe Ch.-A Guillot, The war on terror and the protection of personal data, 1 Montesquieu Law Review (2015), issue 2, available at
http://www.montesquieulawreview.eu/review.htm

The terrorist attacks that took place in Paris in January 2015 have reopened the debate on passenger name records (PNRs), files created by airlines for each flight booked by a passenger – highly intrusive in terms of privacy as they concern data of a personal nature (hereinafter referred to as "personal data") – containing names, methods of payment and, potentially, dietary requirements or health issues, even contact details for the passenger. According to the former chairman of the *Commission nationale informatique et libertés* (CNIL) generalised registration threatens to put "privacy in jeopardy" (1).

Indeed, the war on terror raises the issue of striking a balance between the protection of privacy and the preventive measures implemented without the oversight of a court or an independent authority. The United States rides rough-shod over privacy – the Privacy Act 1974 is very narrow in scope (2) – while the European Union and its Member States consider the protection of personal data as a fundamental right – Article 8 of the Charter of Fundamental Rights of the European Union (CFREU) and Article 16 of the Treaty on the Functioning of the European Union (TFEU). Enshrined by Convention n°108 of the Council of Europe of 28 January 2001 and by the interpretation of Article 8 of the European Convention on Human Rights by the eponymous Court (3) – echoed by decisions handed down in France by the Constitutional Council (4) and the *Conseil d'Etat* (5) – the protection of personal data is governed in particular by Directive 95/46/EC of 24 October 1995, supplemented by Council Framework Decision 2008/977/JHA of 27 November 2008. The scheme, inspired by France's *Informatique & Libertés* (data protection and civil liberties) Law (6), forbids the inclusion of sensitive data – concerning race or ethnic origin, political persuasions, religious or philosophical beliefs, union membership or those relative to drug and alcohol abuse, health or sex life – in data processing and makes such data subject to monitoring by an independent administrative authority – the CNIL in France, the European Data Collection Supervisor (EDPS) for the European Union. Article 29 of the Directive establishes a European group of national authorities – the "G29" – to contribute to the consistent implementation of national provisions. Any person whose personal data has been entered into a database has the right to informed, a right of direct access, a right to have data rectified, a right to object and, more recently, a "right to be forgotten" (7). These are not genuine rights over personal data, but rather personal rights over the processing carried out through a third party (8), even though the *Conseil d'État* recommends "*conceptualising the right to data protection as a right to "informational self-determination", which is to say the individual's right to decide on the disclosure and use of his or her personal data*" (9).

Counter-terrorism co-operation between Europe and the United States must reconcile conflicting approaches, as illustrated by the events surrounding PNRs and the Society for Worldwide Interbank Financial Transactions – Terrorist Finance Tracking Program (SWIFT-TFTP) agreements, which have caused conflict at the very heart of European Union institutions owing, on the one hand, to

differences of perspective on the concessions to be made by the Commission and the Council; and, on the other hand, those to be made by the Court of Justice and the European Parliament (section I). This inter-institutional opposition has prevented the adoption of a European PNR, but France has decided to follow the British example by developing a national PNR. On a European and French level, other measures to prevent terrorism threaten privacy through the widespread surveillance and collection of personal data (section II).

I - Co-operation between the European Union and the United States in the prevention of terrorism versus the fundamental right to protection of personal data

Commission Directive 95/46 defines an *adequate* level of protection to be attained in each Member State and prohibits the transfer of data to any country not providing a similar level of protection. The United States does not offer adequate guarantees - unlike Australia or Canada, with which nations PNR agreements have been adopted (10) - which explains why such long negotiations were necessary to conclude the PNR (section A) and SWIFT-TFTP (section B) Agreements.

A) PNR Agreements

The differences of perspective within European institutions on the legality of the initial agreements concluded with the United States (section (a)) led to the adoption of an Agreement in 2011 which better respects data protection (section (b)).

a - The 2004 and 2007 Agreements

The Aviation and Transportation Security Act 2001 requires airlines operating flights to, from or through the United States to allow the US authorities to access PNR data, on pain of heavy fines (and even not being able to enter American airspace), but European carriers could not then comply with those requirements, being incompatible with EU law and their national legislation.

An initial Agreement was therefore concluded on 28 May 2004, but Commission Decision 2004/535/EC and Council Decision 2004/496/EC implementing that agreement into European law were annulled on 30 May 2006 by the European Court of Justice (11), which nevertheless maintained the effects of the Agreement until 30 September 2006. Following an Interim Agreement of 19 October 2006, which expired on 31 July 2007, a new Agreement was concluded on 23 and 27 July 2007. This provided that air carriers would allow the Department of Homeland Security (DHS) to access data concerning passengers travelling to or from the United States; however, in May 2010, the European Parliament (EP) deferred its vote on the Agreement and called on the Commission to negotiate a new Agreement.

b - The 2011 Agreement

The new PNR Agreement (12) provides that carriers are to provide the DHS with their data in order to prevent or detect terrorist offences or criminal offences related thereto, together with transnational offences punishable by at least three years' imprisonment, or in the face of a serious threat or even if a court orders it. The DHS must filter and delete sensitive data within 30 days - except in cases of threats to a person's life or a specific criminal procedure - and protect all other data from any alteration, destruction or unauthorised disclosure. The DHS must inform the European authorities of serious incidents of invasion of privacy of European citizens. PNR files are stored in an active database for five years then transferred to a dormant database for ten years or

longer in the event of investigations or prosecutions; however, six months after they have been received, the files are "anonymized" (removal of information allowing identification).

The Agreement provides that the DHS may only share the PNRs with Europol, Eurojust or national public authorities investigating the abovementioned offences; thus the use of PNR data runs the risk of extending to uses other than the war on terror. There is cause for concern that a global profiling system infringing individual rights may be set up, the effectiveness of which has not been established: a total of two terrorists have arrested further to the transfer of PNR data and the diversions of aircraft en route to the United States have only concerned instances of similar names (13) and journalists who have been overly critical of US policy (14).

B - The SWIFT-TFTP Agreement

Here too, the EP opposed legislation that infringed the fundamental right to the protection of personal data (section (a)), thus forcing the EU to renegotiate an acceptable agreement (section (b)).

a - History

This Agreement takes its name from the Society for Worldwide Interbank Financial Telecommunication (SWIFT), a Belgian company that processes nearly 80% of international bank transfers. Initially, the US authorities could serve administrative subpoenas on SWIFT in order to obtain data as its servers were located on US soil; however, influenced by data protection agencies (15), SWIFT now operates its processing and transfer of financial messaging data from the Netherlands and Switzerland.

In order to reconcile the war on terror and European law on data protection, an Interim Agreement was negotiated and accepted by Council Decision 2010/16/CFSP/JHA of 30 November 2009. In spite of pressure from the US (16), this initial SWIFT-TFTP agreement was rejected by the EP on 11 February 2010, owing to the lack of proportionality between the rules relative to data transfers, their storage and the security allegedly provided and because European citizens would not have been able to appeal against US authorities in the event of a wrongful use of their personal data as the Privacy Act reserves such actions for American citizens only (17).

b - The Agreement

The new SWIFT-TFTP Agreement (18) provides that financial messaging service providers must, at the request of the United States Treasury Department, transfer data to the latter for the purposes of preventing and detecting terrorism or the financing thereof. Treasury subpoenas must clearly identify the data necessary for anti-terrorist intelligence, investigations or prosecutions. A copy of such subpoenas is sent to Europol, which must verify that the request is admissible; in the affirmative, the request becomes legally binding, obliging the provider to export the data requested to the Treasury Department. Nevertheless, Europol's supervision has been heavily criticised for being ineffective by both the Joint Supervisory Body (19) and the EP (20).

The data thus transferred is deleted after five years, while the information extracted from the data provided is kept for the period necessary for specific investigations or prosecutions.

The Treasury Department can share the data with any State or international organisation, as well as with Europol or Eurojust, but any sharing of information relative to an EU citizen with the

authorities of a third party is subject to the prior agreement of the authorities in the relevant Member State, except where the sharing of data is essential in preventing a serious and immediate threat. The Treasury Department can also share relevant information obtained in the context of the TFTP at the request of Europol, Eurojust or a competent authority in a Member State of the European Union.

The Agreement structures transparency; access, rectification, deletion or blocking rights; the preservation of the accuracy of information; and appeals. Its innovation lays in the monitoring of guarantees by independent supervisory bodies, including a person appointed by the European Commission with the agreement of the United States.

The EP accepted this new, more balanced agreement – and also because the European Banking Federation had stressed the need to return to legal certainty, which the vote of 11 February 2011 had undermined (21).

The PNR and SWIFT-TFTP Agreements continue to be criticised owing to the absence of an independent administrative authority responsible for the protection of personal data in the United States, and they also elicit fears as to excesses that Edward Snowden's revelations have only served to intensify. The fundamental right to protection of personal data has been sacrificed on the altar of the prevention of terrorism, as the Commission has not been able to obtain from the United States that which it secured from Australia or Canada (22).

II – The right to protection of personal data and French and European preventive measures

The establishment of a PNR system, together with other methods for mass, indiscriminate surveillance, are hot topics in the EU (section A) and in France (section B).

A) European Union measures

The development of a European PNR is back on the agenda (section a); however, the annulment of the Data Retention Directive offers food for thought as to the compatibility of systematic preventive measures with the Charter of Fundamental Rights of the European Union (section b).

a – The issue of the European PNR

In November 2007, the Commission presented a proposal for a directive establishing a European PNR for the purposes of preventing terrorism, which was rejected the following year by the European Parliament. The Commission then submitted a new proposal in 2011 (23), but the EP again opposed it on 24 April 2013 – which did not prevent the Commission from funding national PNR projects in 14 Member States (24).

On 11 January 2015, the French Minister of the Interior exhorted the EP to adopt the European PNR, which request was relayed two days later by the President of the European Council who feared that in the absence of such a Directive, 28 national systems would be set up, forming a "*patchwork full of holes*". The change of position on the part of ADLE and S1D MEPs will be crucial to the adoption of the PNR Directive, but many will make their vote subject to the Court's forthcoming decision on the PNR Agreement concluded with Canada (25).
In addition, Directive 95/46 having to be replaced by a Regulation (26) and the Framework Decision by a Directive (27), it would be appear more logical to wait for that legislation to be adopted before envisaging a vote on a PNR Directive which will have to be compatible with it.

b – Other preventive measures

Following the terrorist attacks in Madrid and London, Directive 2006/24/EC of 15 March 2006 on the retention of data was adopted in order to harmonise national measures requiring telecommunications and IT service providers to retain client metadata – and not the content of communications or websites visited – in order to supply the same on request to police or intelligence services.

Two referrals were made to the Court of Justice for a preliminary ruling on the compatibility of the Directive with the CFRE; the Count found that it was incompatible, given that "*[t]hose data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained…*" (ground 27), which constituted an "*interference […] [which was] wide-ranging […] likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance*" (ground 37), all the more so as the Directive covered "*in a generalised manner, all persons and all means of electronic communication*" (ground 57), provided no "*objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use*" (ground 60) and that the retention period had been set without taking account of the usefulness of the retention as compared to the objectives pursued (grounds 63 & 64) (28).

This indiscriminate and disproportionate surveillance differs from Europol's operational measures or the co-operation and exchange of information between law enforcement authorities (29) which target persons who have already been convicted or are strongly suspected in the context of procedures overseen by judges. The strict rules on the protection of personal data – which should be strengthened with the adoption of the proposed Regulation and Directive (30) – that apply to Europol offer satisfactory guarantees, reconciling the war on terror and privacy (31).

B) French measures

France has set up her own PNR system, which is not operational as yet (section a), together with surveillance measures, the most recent of which have only been adopted by the National Assembly – the Senate and the Constitutional Council (to which the President ought to refer the issue) not having decided yet (section b).

a – The French PNR

Article 7 of Law n° 2006-64 of 23 January 2006 on the war on terror authorises the collection of PNR data and Advance Passenger Information (API – passenger data collected by airlines at the check-in stage for any given flight) for international travel to or from third-party States to the EU. This also applies to data directly collected from the machine readable zone on travel documents, identity cards or visas held by passengers travelling with air, sea or railway carriers.

An Order of 19 December 2006 instituted, on an experimental basis, an air passenger record that only concerns passengers aboard direct flights to or from Afghanistan, Pakistan, Iran, Syria and Yemen. However, the experiment mostly revealed "*a lack of rigour in the transmission of data by some airlines and […] multiple errors due to similar names or inaccurate transcriptions of names*" (32).

Furthermore, Article 65 of the *Code des douanes* (Customs Code) allows the Administration to demand PNR data expressly and on an *ad hoc* basis for certain flights.

Article L.232-7 of the *Code de la sécurité intérieure* (CSI – Internal Security Code), resulting from the 2013 Law on military planning, establishes the French API-PNR system (from which sensitive data is expressly excluded) for flights travelling to or from France, as implemented by Decree n° 2014-1095 of 26 September 2014. In an opinion of the same date, the CNIL considered that the guarantees reduced the risk of data protection infringements (33).

b – Extending surveillance

The Law on military planning also allows the intelligence services to create an automated data processing system (Article L. 232-7-I CSI), under the supervision of the *Commission nationale de contrôle des interceptions de sécurité* (CNCIS).

Articles L. 246-1 to L.246-5 CSI require communications operators to retain, for a one-year period, all metadata in order to fulfil requests from anti-terrorist or intelligence services. As this processing of such "traffic data" by those services constitutes purely administrative police operations, so the ordinary courts do not have jurisdiction (34).

The draft Bill on intelligence lists seven public-interest grounds (35) that allow, under future Article L 853-1 CSI, the "*use of technical devices allowing [...] the collection, transmission and recording of computer data transiting through an automated data system or contained within such a system*". These measures will be supervised by the *Commission nationale de contrôle des techniques de renseignement* (CNCTR) – an independent administrative authority replacing the CNCIS – which will submit an opinion to the Prime Minister on the authorization of data collections, except in the event of absolute urgency.

The draft Bill also introduces significant innovations into the CSI, including the guarantee of privacy and – thanks to a parliamentary amendment – the protection of personal data and reference to the proportionality principle (36) (Article L.811-1), the destruction of data extracts or exploitations that are no longer essential (Article L.822-3) and, above all, the possibility of bringing an appeal before the *Conseil d'Etat*, which option is open to any person with a direct and personal interest, the CNCTR or any court making a referral for a preliminary ruling. The *Conseil*'s requests cannot be refused on "military secrets" grounds, even though it will not disclose any information classified as such (Article L.841-1).

It is still too early to know what the law on intelligence will ultimately be; nevertheless, France is attempting to perform a balancing act between the prevention of terrorism and the protection of personal data. Future case-law interpretations of the *Digital Rights* decision, be it in France or the EU, may tip the scales in favour of the latter, at the expense of Articles L.246-1 to L.246-5 CSI. Even if the current trend is towards greater security measures, all is not lost for privacy.

Notes:

(1) A. Türk, *La vie privée en péril. Des citoyens sous contrôle*, Odile Jacob, 2011.

(2) Cf. S. Preuss-Laussinotte, « Bases de données personnelles et politiques de sécurité », *Culture & Conflits*, n° 64, 2006, p. 83; Conseil d'État, *Libertés et numérique*, La documentation française, 2014, p. 72-74.

(3) ECHR, *Leander v Sweden*, Application n° 9248/81, 26 March 1987; ECHR, *Amman v Switzerland*, Application n° 27798/95, 25 March 1998; ECHR, *Rotaru v Romania*, Application n° 28341/95, 4 May 2000; ECHR, *Turek v Slovakia*, Application n° 57986/00, 14 February 2006; ECHR, *S. &*

Marper v United Kingdom, Applications nos. 30562/04 and 30566/04, 4 December 2008; ECHR, *Dimitrov-Kazakov v Bulgaria*, Application n° 11379/03, 10 February 2011; ECHR, *Association "21 December 1989" and others v Romania*, Application n° 33810/07, 24 May 2011; ECHR, *Brunet v France*, Application n° 21010/10, 18 September 2014. The Court nevertheless recognises that the war on terror may justify restrictions on the confidentiality of correspondence and telecommunications (ECHR, *Klass and others v Germany*, Application n° 5029/71, 6 September 1979) or the conservation of certain types of data by the security services (06.06.06, *Segerstedt-Wiberg and others v Sweden*, Application n° 62332/00, 6 June 2006). Cf. A. Petropoulou, *Liberté & sécurité : Les mesures anti-terroristes et la Cour européenne des droits de l'Homme*, Pédone, 2014, p. 443-461.

(4) Decision 2012-652 DC of 22 March 2012, *Loi relative à la protection de l'identité*, para. 8; the Constitutional Council found that judicial police files were constitutional (Decision 2003-467 DC of 13 March 2003, *Loi sur la sécurité intérieure*, para. 17-46), as was the *fichier national automatisé des empreintes génétiques* (FNAEG - automated DNA database) regarding, in particular, the identification of perpetrators of terrorist acts (Decision 2010-25 QPC of 16 September 2010).

(5) CE, Ass., 26.08.11, *Association pour la promotion de l'image*, *Rec.*, p. 505.

(6) Law n° 78-17 of 6th January 1978 as amended by Law n° 2004-801 of 6th August 2004; cf. J. Harivel, « La difficile protection des données à caractère personnel dans une société numérique », *in* I. Bouhadana & W. Gilles (dir.), *Droit et gouvernance des données publiques et privées à l'ère du numérique*, IMODEV, 2015, p.57-64; Conseil d'État, *op. cit.* p.70-76 & 86-87

(7) CJEU, Case C-131/12, *Google Spain SL & Google Inc. v AEPD & Mario Costeja Gonzalez* [2014] ECR 317; Cf. B. Hardy, « La géographie du droit à l'oubli », *R. trim. droit eur.*, 2014, p. 879-897; H. Kranenborg, "Google and the right to be forgotten", *Euro. Data Protec. L. R.*, 2015, p. 70-79; *Conseil d'État*, *op. cit.*, p. 184-189.

(8) Cf. Th. Saint-Aubin, « Les droits de l'opérateur de données sur son patrimoine numérique informationnel », *in* I. Bouhadana & W. Gilles (dir.), *op. cit.*, p. 143-144 ; J. Eynard, *Les données personnelles. Quelle définition pour une protection efficace ?*, Michalon, 2013, p. 141-182.

(9) *Conseil d'État*, *op. cit.*, p. 337; detailed presentation, p. 264-269.

(10) Agreement between the European Union and Australia, 13 September 2011, inter-institutional dossier 2011/0126 (NLE); Agreement between the European Union and Canada, 30 November 2011, inter-institutional 2013/0250 (NLE) - the latter has yet to be approved by the EP, which has referred the issue of the Agreement's compatibility with the CFREU to the ECJ. In the interim, a previous agreement between the EU and Canada, concluded in 2006, remains in force. Furthermore, an agreement between the EU and Mexico is under consideration, while Russia and South Korea have made similar requests.

(11) Joined Cases C-317/04 & C-318/04, *European Parliament v Council of the European Union and Commission of the European Communities* [2006] ECR I-04721. This decision only concerns the legal basis of Decision 2004/535.

(12) Inter-institutional dossier 2011/0382 (NLE), 8th December 2011.

(13) Cf. J.-C. Martin, *Les règles internationales relatives à la lutte contre le terrorisme*, Bruylant, 2006, p. 369-370.

(14) Cf. *Le Monde*, 03.10.12.

(15) Opinion of 27 September 2006, Commission for the Protection of Privacy, Belgium; G.29 Opinion 2006/10, 22 November 2006; EDPS Opinion, 1 February 2001.

(16) Cf. J. Santos Vara, *The Role of the European Parliament in the conclusion of the Transatlantic Agreements on the Transfer of Personal Data after Lisbon*, CLEER Working Papers, 2013/2,

p.16.

(17) Cf. C. Pouliquen, *Le cadre européen de protection des données en matière pénale*, Bruges Pol. Res. Pap., n° 29, 2013, p. 17.

(18) *OJEU*, L.195/5, 27.07.10.

(19) http://europoljsb.consilium.europa.eu.media/111009/terrorist%20finance%20tracking%20program%2028tftp%29%20inspection%20report%20-%20public%20version.pdf (unavailable)

(20) www.europarl.europa.eu/en/pressroom/content/20110314IPR15463/html/SWIFT

(21) Cf. H. Farrell & A. Newman, "The New Politics of Interdependence", *Comp. Pol. Stud.*, 2014, p. 12.

(22) Cf. M.-F. Labouz, « Le nouvel accord sur les données de passagers aériens (PNR) entre l'Union européenne et les États-Unis », *in* E. Saulnier-Cassia (dir.), *La lutte contre le terrorisme dans Le droit et la jurisprudence de l'Union européenne*, LGDJ, 2014, p.269.

(23) COM (2011) 32 final.

(24) Cf. N. Vandystadt, "PNR still divisive in European Parliament", *Europolitics*, n° 4971, 13.11.14, p. 13.

(25) Cf. S. Peyrou, www.gdr-elsj.eu/2015/01/25/cooperation-judiciaire-penale

(26) COM (2012)11 final.

(27) COM (2012)10 final.

(28) CJUE, 08.04.14, *Digital Rights Ireland & Seitleinger*, C-293/12 & C-594/12 ; cf. Conseil d'État, *op. cit.*, p. 197-201.

(29) Cf. C. Castets-Renard, *Droit de l'internet*, Montchrestien, 2e éd., 2012, p. 469-470.

(30) Cf. A. Gattolin *e. a.*, *Rapport d'information fait au nom de la commission des affaires européennes sur Europol et Eurojust*, Sénat, 17.04.14, p. 17-19.

(31) Cf. A. Gutirrez-Zarza (dir.), *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Springer, 2015, p. 95.

(32) Cl. Guerrier, « Passenger Name Record 2012 », 02.07.12, http://www.juriscom.net/wp-content/documents/pnr20120702.pdf

(33) www.cnil.fr/les-themes/deplacements-transports/du-systeme-api-pnr-france/

(34) C. const., 2005-532 DC of 19 January 2015, *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*, recital 5.

(35) National security, essential foreign policy interests and the execution of France's European and international commitments; France's essential economic and scientific interests; prevention of terrorism; prevention of the re-formation or continuation of disbanded groups; prevention of organised crime; prevention of collective violence likely to constitute serious offences affecting the maintenance of law and order.

(36) On the principles of necessity and proportionality, cf. Opinion 01/2014 of the G29, 27 February 2015.