EUROPE

PNR and compensation: how to bring back the proportionality criterion

By Gloria González Fuste, Researcher at the Institute for European Studies (IES) and Law, Science, Technology and Society (LSTS) Research Group of the Vrije Universiteit Brussel (VUB), Belgium, and Paul de Hert, Tilburg Institute For Law, Technology and Society (TILT), The Netherlands, and Vrije Universiteit Brussel (VUB), Belgium.

Introduction

Developments linked to the United States’ demand of Passenger Name Record (PNR) data imposed on European airline companies flying to its territory can be interpreted as a worrying illustration of a series of weaknesses of the European Union’s regime for the protection of privacy and personal data. Major issues that could be cited in this sense are, for instance, the limitations of the system regarding the protection of data originally collected in the context of commercial activities and later processed for law enforcement purposes; the inconsistencies of protection derived from the pillar structure of the E.U., notably concerning the divergent rules applying to data transfers to third countries, and, at a more general level, an extremely serious legitimacy problem (Lodge, 2004), as well as significant accountability concerns, in particular regarding parliamentary accountability (House of Lords, 2007).

This paper specifically focuses on what we believe should be considered one of the main lessons to be learned from the PNR developments: the ineffectiveness of the proportionality criterion in the current E.U. data protection and privacy regime. More concretely, the paper firstly approaches the problem considering its relevance in the field of security-related interferences with private life; secondly, it introduces the notion of compensation, and, finally, it examines the possible contribution of enhanced compensation mechanisms to the effectiveness of the proportionality criterion.

Proportionality assessment by the judiciary

The right to privacy is recognised as a human right in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950 (hereafter, ‘the Convention’). Article 8’s paragraph 1 establishes the principle that public authorities must not interfere with the right to respect for private life, while paragraph 2 accepts that such an interference is possible if in accordance with the law and necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder and crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. Objectives in the public interest can justify an interference with private life, and therefore be protected by Article 8(2) of the Convention, only if they are necessary in a democratic society for the pursuit of legitimate aims and they are not disproportionate to the objective pursued.

Who has the right to determine whether an interference should be considered “proportionate” in the light of a pursued legitimate objective or, on the contrary, 2disproportionate” and therefore in violation of the fundamental right to privacy? Is such a decision to be left exclusively in the hands of the public authorities that establish intrusive security measures? Or should the judicial power have the chance (or the obligation) to proceed to an ultimate assessment of the proportionality of interferences?

Already before the European Court of Justice (ECJ) was confronted with the PNR case (Joined Cases C-317-04 and C-318/04), a tendency could be perceived in the international case law to recognise to public authorities wide discretionary powers in the assessment of proportionality of intrusive security measures. In this sense, the ECJ had underlined in its Österreichischer Rundfunk judgement that, according to the European Court of Human Rights (ECHR), the scope of the national authorities’ margin of appreciation on the proportionality of measures can vary depending on the nature of the legitimate aims pursued and on the particular nature of the interference involved (Joined Cases C-465/00, C-139/01 and C-139/01, §83), implying that the national authorities’ margin of appreciation is especially wide in relation with measures approved for security and anti-terrorisms purposes.

The European Parliament had used as one of its arguments to challenge in front of the ECJ the first E.U.-US agreement¹ on the transfer of PNR data that the agreement itself and its accompanying “adequacy” decision² violated the principle of proportionality, particularly in reference to the quantity of data collected and the retention period foreseen. The ECJ, however, did not have the opportunity to address the argument in its judgement for the PNR case, as it annulled both the Council Decision 2004/498/EC on the conclusion of the agreement, on the one hand, and the Commission Decision 2004/535/EC holding that the US Bureau of Customs and Border Protection (CBP) offered a sufficient level of protection for personal data transferred from the E.U., on the other hand, on formal grounds related to their legal basis.

On the contrary, Advocate General Léger’s did examine the proportionality argument in his Opinion in Cases C-317/04 and C-318/04 (Léger, 2005) and he did it in an extremely interesting, albeit potentially dangerous, manner, which deserves special attention. Indeed, before expressing his views of the validity of the proportionality argument, Advocate Léger’s manifested a series of highly interesting remarks on the scope of the control to be exercised by the ECJ concerning proportionality. He first made reference to the ECHR case law to declare that according to such case law interferences with private life might require a strict judicial control (§ 229); second, he underlined that, also according to ECHR case law, when the interferences are established with
the purpose of national security or fight against terrorism, public authorities enjoy wider discretionary powers (§ 230); finally, he concluded that, in the PNR case, the latter notion shall predominate and, therefore, judicial control could not be strict: recognising to public authorities wide discretionary powers to determine which measures are to be considered proportionate, the judicial control should limit itself to the appreciation of any possible manifest error in such assessment (§ 231). This limitation of the scope of the judicial control marked the Advocate General’s analysis of the proportionality of the measures foreseen in the first PNR agreement, which he concluded to be proportionate taking into account the wide discretionary powers that, in his view, should be recognised to the EC and the Council (§ 246).³

Advocate General Léger’s Opinion can be reasonably perceived as a worrying sign, supporting the view according to which citizens cannot rely on the judiciary to protect them against any intrusive security measures that public authorities might declare proportionate. The progressive self-effacement of the judiciary in its role to assess the proportionality of intrusive measures is especially alarming as it is not yet widely recognised, and therefore certain public authorities might still chose to indulge in increasingly intrusive measures in the belief that, if citizens were to judge them disproportionate, they could always refer to the courts — a conclusion which seems no longer valid.

This should not, however, lead us to believe that the proportionality requirement as recognised in the Convention can simply be considered obsolete. In this sense, and particularly in the context of increasing use of new technologies in the field of intrusive security measures, assessments of proportionality seem more necessary than ever. Ideally, furthermore, such assessments should include a detailed review of all the alternatives in the hands of the decision-makers, taking into account each alternative’s potential impact on individual rights, but also their effectiveness. Analysts have pointed out that courts failing to question the effectiveness of security measures, notably using what has been described as the “deference” argument, cannot be deemed to offer a rigorous balancing between liberty and security, and might therefore be unable to provide meaningful protection of the rights of the citizens (Solove, 2007:5).

PNR and redress

It will be remembered that the demand of PNR data was initially unilaterally imposed by US authorities on air-carries travelling to US territory in the context of the US fight against terrorism. The transfer of data was however later to be legally covered by a series of agreements between the US and E.U. authorities, from the beginning negotiated in difficult discussions (Privacy International, 2004) which did recurrently address the issue of the exact purpose of the collection and the processing of data. Such purpose was to be eventually generally referred to as the “fight against terrorism and transnational crime”. More concretely, the text agreed on June 2007 by the US and E.U. negotiators to replace the Interim Agreement of October 16, 2006 mentions the desire “to prevent and combat terrorism and transnational crime” (Council of the European Union, 2007:1), and its accompanying “US Letter To E.U.” states that “PNR may be used where necessary for the protection of the vital interests of the data subject or other persons, or in any criminal judicial proceedings, or as otherwise required by law” (Council of the European Union, 2007:7).

It could be discussed whether such objectives can legitimate or not massive interferences with private life. It has to be admitted, in any case, that such purpsoes are, if not completely vague, at least very broad, and that they do not explicitly inform the data subject on the exact use of the personal data collected — only on the general objective(s) for such collection. The issue of the exact use of the PNR data has in fact been strongly controversial and heavily discussed in the context of almost continuous revelations on developments on sharing of data, data mining,⁷ data profiling⁸ and other practices taking place in the US territory without initial public awareness (see, for instance: Rotenberg, 2007). Contradictory facts have been revealed regarding the use of PNR data of European citizens as input for the Transportation Security Administration’s Computer-Assisted Passenger Pre-Screening System (CAPPS II) (Kosowski, 2004:17), and, in general terms, there seems to be no clear perception of whether automated profiling based on PNR data takes place or not, nor an unanimous perspective on the eventual lawfulness of such practices (House Of Lords, 2007:11).

Official statements from the US authorities on the processing of PNR data have recurrently been centred on the idea that the collected data are screened against lists elaborated on the basis of data coming from a variety of sources. Two are the main lists publicly acknowledged to be daily used by airline companies: the “No-fly” and the “Selectee” or “Secondary screening” list; a match to the “No-fly” list shall lead to further questioning of the traveller and, possibly, to denied boarding, while a match to the “Selectee” list shall in principle simply result in additional security screening. The use of PNR data to elaborate such lists and the use of algorithms for profiling are generally simply not mentioned, even if it is difficult to imagine why should electronic access to such large amounts of data be required for the sole purpose of screening names against pre-established lists that do not generate real-time risk-assessments.⁹ The reference made in the “US Letter To E.U.” accompanying the text agreed to replace the 2006 Interim Agreement to the retention of data for a period of seven years in “an active analytical database” (Council of the European Union, 2007:10) seems to confirm the interpretation according to which data mining practices take place or are to take place.

In any case, even if the PNR data collected were simply screened against pre-established lists, and even if the lists where configured with perfectly accurate data processed in a perfectly legitimate and careful manner, such screening could also be the direct cause of many travelling problems or “inconveniences”. Indeed, identification and matching techniques present inevitably a degree of fallibility, and their massive implementation can cause a significant number of mismatches and undesired consequences.

On February 20, 2007, the US authorities publicly acknowledged that the screening in the context of PNR data was provoking enough trouble to justify reaction, and decided to launch a specific redress programme, the Traveller Redress Inquiry Programme (TRIP).⁷ The E.U. had actually been backing the establishment of redress mechanisms in the context of the PNR collection since the beginning of negotiations with the US, notably insisting on the possible
representation of European data subjects by European Data Protection authorities. However, and despite efforts to provide a ‘redress’ mechanisms being put in place by US Terrorist Screening Center (TSC) since 2005 [Privacy & Civil Liberties Oversight Board, 2007-1], such mechanisms were originally disregarded by the US authorities responsible for Homeland Security, Inter alia in the name of the need to avoid massive litigation (EPIC, 2006:5).

The scope of TRIP consists basically in the “inconveniences” created by the screening of travellers’ personal data. It is claimed that the programme should be used by those who believe that information held on them is inaccurate, those who have felt discriminated, as well as those who believe they have unfairly been detained or denied entry to the US territory. More concretely, TRIP was introduced as a “single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs — like airports and train stations — or crossing U.S. borders, including denied or delayed airline boarding, denied or delayed entry into and exit from the U.S. at a port of entry or border checkpoint, continuously referred to additional (secondary) screening”.8

Despite its wide general scope, a close examination of what TRIP can really offer to travellers reveals its serious limitations. Indeed, those who might obtain benefit are essentially the passengers that have been more than once referred to secondary screening without any apparent cause. TRIP is presented as an appropriate mechanism to investigate eventual discrepancies in DHS records and to resolve misidentification issues affecting such passengers, who should find help to be able to travel in the future without being subject to systematic secondary screening without apparent cause, even if they are not to receive any compensation for the “inconveniences” already suffered. For the other travellers, TRIP shall be of little use or benefit.

Compensation as a tool contributing to proportionality

Compensation mechanisms should be structurally different, in order for them to play a significant role in the deployment of security measures. Compensation mechanisms should not only be easy to use and adequately wide in scope, but also generous enough to ensure that public authorities take the required care in assessing the consequences of all intrusive security measures before launching their wide implementation. They should acknowledge all related “inconveniences” caused by security measures, not only for the person whose data have been inaccurately processed, but also for others who might have suffered any related consequences, such as accompanying travellers.

The amounts provided in case of undue inconvenience should be significant enough to dissuade public authorities of implementing measures that are not the best possible technological solution available, allowing them to quantify at least partially the cost that their decisions can have on data subjects. More conveniently, the economic consequences of compensation mechanisms should be an incentive for the responsible public authorities to play a proactive role in the development of technologies and working methods that minimise interferences with privacy. Paths for such development are numerous: generalisation of access on strict “need-to-know” basis, reduction of identification errors, limitation of access, or improvements in the security of data can be named. The ultimate objective of compensation mechanisms should be to oblige the responsible authorities to recognise, in the use of their discretionary power, the real importance of such discretion and the need to be able to justify their choices. In this sense, it should never be forgotten that a significant number of what are generally presented as simple technical choices can hide political or at least not merely technical decisions.8

Compensation is not an unknown notion in the field of E.U. data protection. Indeed, compensation is notably foreseen by Directive 95/46/EC (the ‘Data Protection Directive’)9, as well as by the more recent Directive 2006/24/EC (the ‘Data Retention Directive’).11 Conceptually, however, we shall distinguish the compensation foreseen by such provisions, which is essentially a sanction for non-compliance, and compensation as it should be implemented in order to have a real impact in issues such PNR transfers, in which the multi-layered nature of the transfers and confidentiality of processing undermine the relevance of any simple compliance checks with legal provisions. In this perspective, the design of compensation mechanisms should preferably take inspiration in the measures provided by Regulation (EC) No. 261/2004 establishing common rules on compensation and assistance to air passengers in the event of denied boarding and of cancellation or long delay of flights — although the measures should be adapted to the particular nature of the reason causing the inconvenience.

An example of the potential impact of compensation mechanisms might be found in the field of discriminatory practices related to the use of personal data. If we consider that “data-mining initiatives based on broad terrorist profiles that include group characteristics such as religion and national origin may constitute a disproportionate and thus arbitrary interference with the right to privacy” (Scheinin, 2007:9), the essential question that needs to be answered is how and when is the assessment of the proportionality of such initiatives going to take place, particularly taking into account the already mentioned lack of judicial assessment of proportionality.

In our view, a well-designed compensation mechanism should contribute to such assessment by considering discrimination as a factor to multiply compensation. This multiplying power seems fully justified in the light of studies in the field of profiling practices according to which the negative effect on the citizens subject to such practices is amplified by the believe that characteristics such as race or religion played a role in the law enforcement officer’s decision (Moedl, 2008:19). Incrementing compensation when the “inconvenience” appears to be linked to discrimination should eventually force the public authorities to ensure that the practices they establish are not discriminatory, nor felt as such.

It is true that compensation mechanisms do not directly aim at resolving the cause of the “inconveniences” suffered. It is important to notice, however, that some approaches that can be presented as directly addressing the cause for misidentification and other “inconveniences” actually fail to do so. Indeed, it is sometimes believed that a possible solution to ensure the protection of personal data in the context of the processing of PNR data would be to guarantee the right to access and rectification to the data used for creating watch
lists such as the "No-fly" or the "Selectee lists". This idea neglects the importance of the practical obstacles that difficult the exercise of such rights in this specific context, and, furthermore, it does not take into account the fact that accuracy of data does not provide any assurance of lack of "inconveniences".

Regarding the practical obstacles, it can be recalled that one of the initial criticisms addressed at the TRIP programme pointed out that better solutions would require to make applicable the US Privacy Act of 1974 to all the data used for screening PNR data. The "US Letter To E.U." accompanying the text agreed to replace the 2006 Interim Agreement foresees that disclosure of data should be ensured in accordance with the Privacy Act and US Freedom of Information Act (FOIA), but at the same time recalls that the Department of Homeland Security (DHS) may in some circumstances "deny of postpone disclosure of all or part of the PNR record" (Council of the European Union, 2007:10), providing therefore little reassurance on the real utility of the possibility to request disclosure. Most notably, the accuracy of data held cannot guarantee per se that its interpretation does not lead to inappropriate measures (House of Lords, 2007:13), making compensation mechanisms suitable even in case of the eventual possible access to and rectification of personal data.

It needs to be noted that a major advantage of an easy to use, wide in scope, generous and, therefore, popular compensation mechanism would be its contribution to the gathering of information on the "inconveniences" related to travellers screening. With the aim of rendering such collection of information particularly useful, the coordinated participation of Data protection Authorities should be encouraged, as they could centralise information and share it at European level. Information would be of use to encourage general awareness of data processing practices, therefore contributing to public debate on security measures. Lack of information to passengers has already been acknowledged as a crucial problem related to the PNR transfers, and seems to be a persistent problem despite the insistence of Data Protection Authorities in recalling to airline companies their obligations (Art. 29 Working Party, 2007).

**Conclusion**

Compensation mechanisms should be conceived and implemented as a tool to monitor the development of those security measures that are currently benefitting from the wide discretionary powers left by the courts in the hands of public authorities. The need for such monitoring is to be linked to the necessity of maintaining the proportionality criterion as an effective and fully operative criterion, and is reinforced by the idea that wide use of new technologies for the purpose of surveillance cannot be expected to be totally unproblematic. In this sense, compensation has been linked to the "many failures" that "can be foreseen" as new technologies are implemented for surveillance purposes (Royal Academy of Engineers, 2007:8).

The mechanisms as envisaged in this paper will offer potentially many more benefits than mere individual redress. Their efficiency in generating collective benefits, however, relies ultimately on the generosity of the compensation provided for each and every individual suffering 'inconveniences'. The economic importance of the compensation appears indeed to be a key factor to recall to the responsible authorities the difference between a justified trade-off between security and liberty, on the one hand, and an imposed unnecessary interference with private life, on the other hand.

**References**


Joined Cases C-465/00, C-138/01 and C-139/01, Österreichischer Rundfunk (2003), ECR I-4989.


1 Concluded between the E.U. and the USA on May 28, 2004.
3 « L’ensemble de ces garanties nous conduisent à considérer que, eu égard à la grande marge d’appréciation qui doit, selon nous, être reconnue en l’espèce au Conseil et à la Commission, l’ingérence dans la vie privée des passagers aériens est proportionnée au but légitime poursuivi par le régime PNR » (underlined by the author) (Léger, 2005:5-64).
4 Data mining can be described as “the use of advanced algorithms to trawl through huge databases to discover someone or something matching that profile” (House of Lords, 2007:10).
5 Data profiling can be defined as “the determination of characteristics or combinations of characteristics which might identify someone or something as potentially worth investigation” (House of Lords, 2007:10).
6 If verifying the presence of a name in a list or an identity was the exclusive purpose of the collection, this could be probably be done collecting solely the data known as Advanced Passenger Information (API), which is machine readable data collected at checking or boarding and includes the name of the passenger. In the absence of profiling and data mining intentions, the need for data such as ‘travel agency’ and ‘baggage information’ is difficult to understand.
7 In April 2008 the DHS Privacy Office had already publicly recognised that “Inclusion of a robust, effective redress process should be an essential element of any current or future federal screening program” (Cooney, 2006:iv).
8 More information on TRIP can be found at www.dhs.gov/xtripsac/programs/gc_1169678919018.shtm.
9 It is the case, for instance, in choices regarding systems for matching names, as even if all systems might inevitably be prone to errors, they might be prone to errors differently: “Systems designers must perform a trade-off between false positives and false negatives generated by a system – as one type of error decreases, the likelihood of the other type tends to increase” (Cooney, 2006:11).
10 In Article 23: “1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered; 2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.” The provision is referenced to in Article 15(2) of Directive 2002/58/EC (the ‘e-Privacy Directive’).
11 In Article 13.
Legislation and Guidance

International: New international privacy standards may offer the solution to global data privacy problems .......................................................... 3
Europe: PNR data and compensation: how to bring back the proportionality criterion .......................................................... 4
How Freedom of Information is re-writing the definition of personal data & privacy within the United Kingdom ........................................ 5
United States: Managing your data processors - legal requirements and practical solutions .......................................................... 6

Personal Data

Europe: Article 29 Working Party issues guidance on the definition of personal data .......................................................... 15

News

Legislation and Guidance

Asia Pacific: Australia Privacy Act review – security breach notification ....... 8
United States: Multinational fined for cross-border data transfer ............. 9

Personal Data

International: Privacy International privacy ranking of internet service companies – interim report released ...................... 16
United States: Electronic voting – no secrecy for voters in Ohio ............. 17
Ireland: Data Protection Commissioner raids text marketers .............. 18