D.2.5. Recommendation Report:
Situating Privacy and Data Protection in a Moving
European Security Continuum

Deliverable submitted March 2011 (M36) in fulfillment of requirements of the
FP7 Project, Converging and Conflicting Ethical Values in the Internal/External
Security Continuum in Europe (INEX)
D.2.5. Recommendation Report: 
Situating Privacy and Data Protection in a Moving 
European Security Continuum 

INEX Work Package 2 (Lead beneficiary: VUB) 

 Contributors: 

Gloria González Fuster, Paul De Hert and Serge Gutwirth
Introduction

Be it in the name of security, in the name of mobility control, or in the name of these two ‘twin objectives’,\(^1\) the automated processing of data related to individuals has been and is still being strongly promoted by the European Union (EU). Practices supported by EU institutions range from the creation of large-scale databases to store of information that can include biometric data\(^2\) to the adoption of legal instruments that impose the massive processing of information on everyday activities of all individuals moving across the EU territory, on their communications or their financial transactions, but can also involve the transfer of data to specialised EU agencies, such as Europol or Eurojust, or to the ‘competent authorities’ of third-countries, to mention a few examples.

There is no doubt that these measures have an impact on fundamental rights. But which are the fundamental rights more deeply affected by them? And how should these rights be activated to ensure the effective protection of individuals and of democratic societies? A series of critical elements must be highlighted in order to address the legal dilemmas arising in this area. The present paper reviews them in the light of the results of the research undertaken by Work Package 2 of the Converging and conflicting ethical values in the internal/external security in continuum in Europe (INEX) project,\(^3\) under the title “Cross-border legal dilemmas of the internal/external security continuum”.\(^4\)

Recommendations

1. Data processing needs to comply with the requirements of the Council of Europe regarding the right to respect for private life and the EU legal framework for personal data protection. As repeatedly recalled by the European Court of Human Rights (ECtHR), storing information about persons can constitute an interference with their right to respect for private life as established by Article 8 of the European Convention of Human Rights (ECHR). This implies that any decision to record data on individuals is only acceptable if it pursues a legitimate interest, if it is taken in accordance with the law and if it is necessary in a democratic society. Additionally, the EU legal framework foresees a series of safeguards for the processing of any data that can be legally qualified as ‘personal’, i.e. data that refers to identified or identifiable individuals. Since the entry into force of the Lisbon Treaty in 2009, the protection of personal data defined in such terms has been formally elevated to the status of fundamental right in the EU. Therefore, it is now more important than ever for EU institutions to ensure that any initiative leading to the

---


\(^2\) As, for example, Eurodac or the non-yet operative Visa Information System (VIS) or Schengen Information System (SIS) II.

\(^3\) More information on the INEX project, funded by the European Union, can be found here: [http://www.inexproject.eu/](http://www.inexproject.eu/).

\(^4\) See also, for specific policy recommendations regarding the Schengen Information System (SIS): Parkin, Joanna (2011), Policy Recommendation Report: The Intersection between the Schengen Information System and the EU Rule of Law, INEX Deliverable D.2.4, INEX Project, Brussels.
processing of personal data respects all the core elements of this emergent right, as described by Article 8 of the EU Charter of Fundamental Rights.\(^5\)

However, the current importance of the right to the protection of personal data should not lead to disregard the fact that the obligation to comply with Article 8 of the ECHR (also echoed in Article 7 of the EU Charter) remains as relevant as ever, and that the scope of application of this right can cover the processing of data not relating to any identified or identifiable individual, but to ‘unidentifiable’ people’s movements, activities, behaviours, or their environment. Practices that do not constitute a personal data protection issue *strictu sensu* can represent an infringement to the right to privacy – and vice versa. *EU institutions should never limit the assessment of the impact on fundamental rights of security measures that comprise the processing of personal data to an assessment of their compliance with data protection law.*\(^6\)

2. The mere storage of data, as well as the broadening of access to existing databases, can also have other consequences on fundamental rights and notably constitute stigmatisation and discriminating measures.\(^7\) The possible negative impact of processing data about individuals is not limited to infringements of the right to respect for private life or the right to the protection of personal data. Imposing some data processing practices on some categories of individuals can have important consequences in terms of stigmatisation and discrimination of the affected individuals.

The case law of the highest European courts has highlighted this fact. Strasbourg’s ECHR underscored in the judgement for the *S and Marper v. United Kingdom* case\(^8\) that retaining biometric data of innocent people in a database used for criminal identification purposes presented risks of stigmatisation, in particular as individuals entitled to the presumption of innocence were being treated in the very same way as convicted persons. The Court noted that, although the retention of data of innocent did not equate exactly with the voicing of suspicion, the innocent’s perception of not being treated as innocent could be heightened as their data was stored indefinitely, just like the convicted persons’ data.\(^9\)

In a different context, Luxembourg’s European Court of Justice (ECJ) has observed (in the *Huber* judgement)\(^10\) that the use for crime fighting purposes of a system of processing for personal data of non-national EU citizens, in the lack of equivalent data processing system for nationals, is contrary to the principle of non-discrimination of EU-citizens. In his Conclusions for the case, Advocate General Poiares Maduro had pointed out that the coexistence of different data processing practices for nationals and the other for non-national EU citizens casted an “unpleasant shadow” over non-national EU citizens.

---


\(^7\) On this point, see notably: González Fuster, Gloria, Paul De Hert, Erika Ellyne and Serge Gutwirth (2010), *Huber, Marper and Others: Throwing new light on the shadows of suspicion*, INEX Policy Brief No. 11, Centre for European Studies (CEPS), Brussels, June, Brussels.

\(^8\) *S. and Marper v. The United Kingdom*, Applications nos. 30562/04 and 30566/04, European Court of Human Rights, Judgement of 4 December 2008 (hereafter, *Marper*).

\(^9\) *Marper* § 122.

\(^10\) *Huber v. Germany*, European Court of Justice, Case C-524/06, Judgement of 16 December 2008.
Specific data processing practices can also put under pressure other fundamental rights, such as the freedom of expression and the freedom of religion, especially if they rely on religious or political characteristics as parameters or target particular groups or activities, as well as the principles of criminal law, including the presumption of innocence. EU institutions must therefore imperatively assess the impact of security measures taking into account the full range of fundamental rights and legal principles that could be affected.

3. Third country nationals are currently particularly exposed to the negative impact of EU-supported data processing practices. Fundamental rights such as the right to privacy and the right to the protection of personal data are not exclusively directed towards the protection of EU citizens, but generally of ‘everyone’, and, thus, also of third country nationals. The rights of the latter, however, are particularly vulnerable in face of the persistent deployment of EU-supported data processing measures, ranging from the creation of large-scale information systems (the so-called ‘digital borders’ of the EU) to the reliance on modern surveillance technologies for the control of EU’s external ‘physical borders’, and passing through the pressure to expand the powers of the European Agency for the Management of Operational Cooperation at the External Borders (FRONTEX). A current trend towards the progressive interconnection of the ‘digital borders’ among them and with systems of surveillance of ‘physical borders’ represents a major challenge in this area. In this sense, any progress towards the interoperability of information systems (including, notably, their possible management through a single EU agency) cannot be accepted without the taking into account of its consequences on the right to privacy, the core principles of data protection and the need to restrain all its negative effects. Just as EU institutions acknowledge that fundamental rights of EU citizens must be placed at the centre of the development of an Area of Freedom, Security and Justice (AFSJ), they should also explicitly place the individual’s fundamental and human rights at the core of border management.

4. Lack of privacy and data protection are too often the result of EU institutions imposing data processing practices without simultaneously substantiating the necessary safeguards. The particular dynamics of EU integration have been facilitating the proliferation of situations in which data processing measures are adopted and implemented while effective privacy and personal data protection are deferred to another moment, delegated to different actors, or both postponed and handed over to another level of decision-making. And this can have dramatic consequences for the effective insurance of fundamental rights.

The problems with Directive 2006/24/EC (known as the Data Retention Directive) can be regarded as an example of this phenomenon. Under the Data Retention

---


Directive, telecommunication companies are required to store communication traffic data for a period of between six months and two years. The circumstances in which access to such data can take place and the use of the retained data are not defined, but left to Member States discretion. It is precisely in this area that most of the (many) data protection concerns raised in the implementation of the Data Retention Directive have appeared.\(^{14}\)

Problems referring to the implementation of the national measures taken in relation with the Third Money Laundering Directive\(^{15}\) must also be mentioned. This Directive imposes on the regulated sector a duty to report to the national Financial Intelligence Unit (FIU) any transactions and activities that seem to involve funds which are the proceeds of criminal activity, in the form of reports. In the United Kingdom, these reports are entered into a database\(^{16}\) that has been repeatedly criticised as not ensuring basic personal data protection requirements, notably because of the long retention periods imposed on all reports, even those where the ‘suspicious’ dimension of the activity or transaction have not been confirmed, and the wide access granted to different actors to its content.\(^{17}\) In different Member States, data protection issues have emerged due to the wide derogations and exemptions to standard safeguards granted in the name of the fight against terrorism, which is officially the general purpose of legislation in the area, and which contrast with the fact that the vast majority of flagged transactions and activities are unrelated to counterterrorism.

Another example of extremely risky lack of precaution from EU institutions can be found in the European Commission’s Communication with its latest proposal for the use of travel data of individuals flying to and from the EU for sake of counterterrorism and the fight against serious crime.\(^{18}\) In its Communication, the European Commission goes as far as to admit that the whole proposal is based on a definition of ‘serious crime’ that in different Member States can include minor offences that make the proposal contrary to the principle of proportionality, only to add that said Member States are entitled to exclude such minor offences from the scope of application of the transposing legislation.\(^{19}\)

The European Commission adopted in 2010 a strategy for ensuring that the fundamental rights provided for in the EU Charter of Fundamental Rights become reality, and, in its context, notably committed to remind Member States, where necessary, of the importance of complying with the Charter when implementing EU law.\(^{20}\) When legal instruments leading to data processing of a magnitude as those described are adopted, however, such a reminding effort might be insufficient in order to guarantee that the right to privacy and the right to personal data protection of the individuals are satisfactorily guaranteed. *EU institutions should support data processing practices of this significance only if they meet all necessary requirements*

---

\(^{14}\) In three Member States, the Constitutional Court has annulled the national law transposing the Directive.


\(^{16}\) Known as ELMER and maintained by the Serious Organised Crime Agency, (SOCA).


\(^{18}\) COM(2011) 32 final, op. cit.

\(^{19}\) Idem, pp. 15-16.

in terms of necessity and proportionality and, in such case, if they are to be deployed together with, and not while waiting for, clearly defined and adequate safeguards.

5. Profiling is an exceptionally intrusive data processing method requiring explicit justification. Profiling as a contemporary security practice is a data processing technique requiring the analysis of vast amounts data in order to identify patterns that seem to match the description of a threat, and, based on the patterns elaborated through this procedure, select items or individuals.\(^{21}\) It has infiltrated EU security through the fields of the fight against money laundering\(^{22}\) and the use of travel information of individuals travelling by plane for law enforcement purposes. Relying on this technique to pursue security objectives has particular implications from a human rights perspective.

The Council of Europe’s Committee of Ministers recently adopted a Recommendation on the protection of individuals with regard to the automatic processing of personal data in the context of profiling in which it is made clear that profiling has its own risks.\(^{23}\) According to this Recommendation, profiling can have a significant impact on individual’s rights and freedoms of the people affected because it puts them in predetermined categories, very often without their knowledge, and because the profiling technique is generally invisible and thus uncontrollable by the subject concerned. The Recommendation explicitly recognises that the impact of profiling is unaffected by whether the data originally processed refers to identified persons or are based on ‘anonymous’ observations, even though it focuses on providing guidance for the processing of personal data defined as relating to an identified or identifiable individual.\(^{24}\)

In any case, it is not enough for data processing practices relying on profiling to meet the requirements of data protection law regarding issues such as the duration of the storage of data, the data subject’s rights in relation with the data processed, or independent monitoring. The very reliance on the technique of profiling needs to be justified, necessary in a democratic and in accordance with law, this latter idea including obligations in terms of transparency, and thus of publicity of the variables used to established patterns and to flag individuals.

6. Crime prevention is an interest that can justify interferences with the right to respect for private life, but, when used as such, must be interpreted restrictively. Contemporary security practices, and especially those related to profiling and data mining, are marked by a trend towards prevention that in some cases appears to slide towards anticipation. Less concerned with avoiding the commission of future crimes than with taking in advance measures that could be useful if a crime was to be committed (and thus playing less a ‘pre-emptive’ function than a sort of ‘preparatory’

---


\(^{22}\) See, for instance, Directive 2005/60/EC, already mentioned.

\(^{23}\) Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, adopted on 23 November 2010.

\(^{24}\) This can be explained by the fact that the legal instrument serving as a reference for the Recommendation is the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 28 January 1981, European Treaty Series No. 108 (known as ‘Convention 108’).
role), they can be described as following logics of ‘radical prevention’ that encourage the adoption of measures just in case a crime is committed – one can think, for instance, of the storage of DNA data of innocent individuals, unsuspected of any crime, in criminal identification databases.

The linkage between crime-fighting and crime prevention is far from being new, but its translation in uses of modern information technology, offering unprecedented capabilities in terms of data collection, storage and processing, raises questions that need to be carefully considered. These relate to the very principles of criminal law, as well as to other rights, include the right to privacy. Although Article 8(2) of the ECHR does mention “the prevention of disorder or crime” as one of the interests that can legitimate be invoked by States to justify an interference with the right to respect for private life, it must be taken into account that all restrictions to human rights must be interpreted restrictively and, thus, “the prevention of disorder or crime” cannot be understood in this particular context as covering also cases where the link between the interference and the (strictly defined) prevention of crime is unclear or inexistent.

The ECtHR has not yet provided exact guidance on when should the storage of data related to individuals be justified in the name of crime prevention, and when it should not. Nevertheless, circumscribing the role of crime prevention to democratically acceptable limits must be a priority when considering any measures that amount to an interference with the right to privacy.

7. Public data are not freely available data. There is a trend in the security field to increasingly consider, or even support, the processing of so-called ‘open source data’. This category of data would refer to data that is ‘publicly available’, in the sense of not intended for or restricted to a particular person, group or organisation, for instance by being accessible through the Internet. The expression appears to have originated in the United States (US), where the military has advocated for the systematic collection, processing and analysis of information obtained through such data in response to intelligence requirements.

From the US, it is now reaching EU security intelligence. In the EU legal framework, however, the notion of ‘open source data’ has no meaning; it does not refer to any particular type of data, and its use can create dangerous confusion. What is relevant from a European (legal) perspective is that the processing of any data, including the data that could be regarded as ‘publicly available’ in the sense of ‘not confidential’, can potentially constitute an interference with the right to respect for private life of individuals as guaranteed by Article 8 of the ECHR, and thus is only permissible under strict conditions.

---


26 Hayes, Ben (2011), Spying in a see through world: the “Open Source” intelligence industry, Statewatch Analysis, N° 119, p. 1.

27 Hayes, Ben (2011), Spying in a see through world: the “Open Source” intelligence industry, Statewatch Analysis, N° 119, p. 2.

28 The EC is funding through FP7, for instance, a project for the design of a Versatile InfoRmation Toolkit for end-Users oriented Open-Sources exploitation (VIRTUOSO).

29 It can, on the contrary, conflict with other existing legal notions established in the Member States. For instance, the Spanish legal framework regulates the use of data from ‘publicly accessible sources’ (‘fuentes accesibles al público’), but explicitly limits the number of sources that can be considered as such, and the Internet is not one of them.
The ECtHR has made it clear that, even though its name might seem to suggest otherwise, the right to respect for ‘private life’ as guaranteed by Article 8 of the ECHR is not unconcerned with the respect for ‘public life’. The European right to respect for private life is not about the protection of any ‘private’ sphere, nor ‘private’ communications, or ‘private’ spaces, or even the places and acts for which one might have any ‘expectations of privacy’. Additionally, all data, including ‘publicly available’ data, can potentially fall under data protection legislation, which defines ‘personal data’ solely taking into account whether the data refers to an identified or identifiable person, and thus regardless of whether the data is disclosed or undisclosed, accessible or inaccessible, private or public. The use of the notion ‘open source data’ to drive the processing of data related to individuals is, from a European standpoint, fundamentally misleading and should thus be avoided.

8. ‘Privacy by design’ is a policy notion with international appeal that, in order to be incorporated into the EU legal framework, needs to be carefully translated into EU legal terms. The ‘privacy by design’ motto is more and more present in EU policy documents. It originated in Canada and has been spreading globally thanks, notably, to the support of the international community of data protection authorities and privacy commissioners. It seems to enjoy also some backing from the industry.

The European Commission has been considering the possibility of introducing the notion of ‘privacy by design’ in the upcoming legal instrument for a comprehensive EU legal framework on personal data protection, even if it has not yet expressed clearly how it could be translated into legal terms. The European Data Protection Supervisor (EDPS), who has recurrently advocated in favour of promoting this notion, envisages it as an element of accountability and considers it refers to the integration of data protection and privacy from the very inception of new products, services and procedures that entail the processing of personal data.
The introduction of the ‘privacy by design’ approach into EU legislation on personal data protection raises two crucial questions that have not been satisfactorily addressed yet:

a) the relation between the notion of ‘privacy’ in ‘privacy by design’ and EU privacy and personal data protection: over the recent years, the EU has progressively configured the protection of personal data as an autonomous fundamental right, different from the right to privacy. The idea of ‘privacy by design’, however, has been developed mainly outside the EU, by non-EU data protection authorities and privacy commissioners, as well as by multinational companies, who have conceptualised it by emphasising that it allows the embedding of something that they designate as ‘privacy’ into different practices. But what ‘privacy’ is exactly being referred to? Is it what the EU legal framework currently regards as ‘privacy’, or the peculiar ‘informational privacy’ that the global ‘privacy community’ commonly hides under such term? If the latter option appears to be more accurate, then ‘privacy by design’ might as well just be an unlucky term to refer to ‘data protection by design’. In this case, it would be more appropriate to speak about ‘data protection by design’, since privacy covers both a broader and a narrower scope than data protection: privacy violations can occur without any violation of data protection law, and not every violation of data protection is a violation of privacy;

b) the possibility to incorporate into a legal instrument an organisational notion that is based on the idea of ensuring the respect of the legal framework: it is undisputed that those who are responsible for the processing of personal data should comply with the pertinent data protection laws. And it is certainly beneficial to encourage them to remember that they have to do so before it is too late. What could be dangerous, nonetheless, is that the legislator incorporates into mandatory rules a notion that some tend to interpret as an invitation not to embed into their own practices the requirements of privacy and personal data protection as defined by legal and judicial practice, but as an enticement to reinterpret the content of privacy in the light of their own interests. ‘Privacy by design’ cannot be perceived as meaning ‘design your own privacy’, but should focus on the search of ways paths to satisfactorily articulate legal requirements and non-legal practices.

EU institutions need to urgently clarify the relation between ‘privacy by design’ and the EU rights to privacy and personal data protection.

9. The review of Data Protection Directive is a major opportunity to restate the importance of personal data protection and increase its effectiveness, including in relation to cross-border data flows.

In the upcoming years the EU is to establish a comprehensive personal data protection scheme covering all areas of EU competence, and, at the same time, be a driving force behind the development and promotion of international standards for personal data protection and in the conclusion of appropriate bilateral or multilateral instruments.

---

36 For instance, it has been asserted that: “Privacy by Design refers to the philosophy and approach of embedding privacy into the design, operation and management of information technologies and systems, across the entire information life cycle” (Resolution on Privacy by Design, op. cit.).

37 Anchored in Art. 8 ECHR and Art. 7 of the EU Charter.


These two objectives (namely, reinforcing personal data protection inside and outside EU territory) cannot be envisioned independently. The work towards a comprehensive personal data protection for all areas of EU competence has been marked by the publication by the European Commission of a Communication taking as a starting point the possible review of Directive 95/46/EC (known as the Data Protection Directive). The Data Protection Directive had been originally drafted at a time when the very possibility for EU institutions to legislate on issues touching upon the protection of fundamental rights was debated. The current challenge for EU institutions is to move decidedly from the provisions originated in such a frame of reference to a new instrument that must be fully consistent with the entry into force of the Lisbon Treaty, which formally establishes the right to the protection of personal data as an autonomous fundamental right and obliges the EU legislator to secure it all over EU competence.

In this context, regulating cross-border transfers of personal data triggers a significant number of legal dilemmas. The most critical concerns the need to establish rules on applicable law that ensure the direct applicability of the Member States’ data protection legislation even when personal data are processed outside the borders of the EU, as soon as there is a justified claim of applying EU law. This is crucial for EU personal data protection to be effective. Existing rules on applicable law are not only complex, but also unable to provide any assurance to EU citizens on the fact that EU data protection will be applicable to data processing situations brought about their daily on-line or off-line activities. By revising such rules, the EU legislator would not only contribute to the effectiveness of personal data protection inside the EU, but would also strategically reinforce its position and credibility for the development and promotion of international standards for personal data protection and in relation to the conclusion of any international agreements regarding data protection safeguards for non-covered data transfers.

10. The trend to positively integrate fundamental rights into EU political discourse should not divert attention from the fact that, at least in some cases, these rights must play a countering role. The much criticised portraying of security and liberty as values opposed in a zero-sum game (sometimes expressed in terms of oppositions of security vs. privacy) seems to be a thing of the past. Currently, the message coming out of EU institutions could be summarised as being that security and fundamental rights can only coexist and develop in a series of win-win situations, that they go “hand in hand”. The reliance on this kind of imagery has certainly its positive effects, such as emphasising the potentially constructive contribution to EU policies of actors directly concerned with fundamental rights’ protection and constantly involved in a dialogue with the EU legislator, like the EDPS. Nevertheless,

---

41 European Data Protection Supervisor (2011), op. cit., p. 25.
it can also distract from the fact that fundamental rights are not expected to push always in the same direction as security and mobility control concerns. The right to privacy, but also the right to the protection of personal data, just as any other fundamental right, carry by definition an amount of resisting strength. It might be a power to oppose certain intrusive practices, as with the right to privacy, or a force to impose on those implementing data processing measures a series of obligations, as with the right to the protection of personal data. Deprived of such a function of resistance, fundamental rights are ultimately transformed into mere enabling factors of policies that, at least in some circumstances, they are supposed to be able to transform.
References


González Fuster, Gloria, Paul De Hert, Erika Ellyne and Serge Gutwirth (2010), Huber, Marper and Others: Throwing new light on the shadows of suspicion, INEX Policy Brief No. 11, Centre for European Studies (CEPS), Brussels, June, Brussels.


González Fuster, Gloria, Serge Gutwirth and Paul De Hert (2009), Analysis of the value dimensions of European law relevant to current and anticipated challenges of the internal/external security continuum, INEX Deliverable D.2.2, INEX Project, Brussels.


Hayes, Ben (2011), Spying in a see through world: the “Open Source” intelligence industry, Statewatch Analysis, N° 119.


Microsoft (2010), *Privacy by Design at Microsoft*, November.

