available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Report

Security and DNA data transfer within the EU

The Prüm decision – An uncontrolled fishing expedition in 'Big Brother' Europe

Sylvia Kierkegaard

International Association of IT Lawyers, Denmark

ABSTRACT

The enlargement of the European Union and the abolition of the borders between the Member States have led to security challenges. In the context of improving security, recent initiatives have focused on the exchange of law enforcement information with effect in 2008 under the "availability" principle. This principle of availability was introduced in the Prüm Treaty, also known as Schengen III. The core element of the treaty is the creation of a network of national databases to promote the exchange of information between law enforcement authorities. In particular, reciprocal access is given to Contracting States' national databases, containing DNA profiles, fingerprints and vehicle registration data. Although this initiative started as a multilateral agreement, a small group of influential countries led by Germany has successfully twisted the arms of other EU countries into integrating the provisions of the agreement into the legislative framework of the European Union under the Third Pillar. The treaty has been incorporated into a Council Decision binding on all EU member states. While the treaty represents a progress in the field of co-operation against crime, the implications of this treaty are far reaching. It raises privacy and data protection issues which will affect all EU citizens, primarily due to the absence of common legally binding data protection standards.

1. Introduction

Criminals do not respect borders. The enlargement of the European Union and the abolition of the borders between the Member States have led to security challenges. In the context of improving security, recent initiatives have focused on the exchange of law enforcement information with effect in 2008 under the "availability" principle.

The principle of availability is defined in the 2004 Hague Program for strengthening freedom, security and justice in the European Union of November 2004 as the possibility whereby "a law enforcement officer in one Member State of the Union who needs information in order to carry out his duties can obtain it from another Member State and that the law enforcement authorities in the Member State that holds this information will make it available for the declared purpose, taking account of the needs of investigations pending in that Member State".[1] Under this principle, full use should be made of new technology and there should also be reciprocal access to national databases, while stipulating that new centralized European databases should be created only on the basis of studies that have shown their added value.

This principle of availability was introduced in the Prüm Treaty, also known as Schengen III. The core element of the treaty is the creation of a network of national databases to promote the exchange of information between law enforcement

[1] The European Council sets 1 January 2008 as the deadline for achieving this objective in the Hague Program.

0267-3649/$ – see front matter © 2008 Sylvia Kierkegaard. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.clsr.2008.03.002

authorities. In particular, reciprocal access is given to Contracting States' national databases, containing DNA profiles, fingerprints and vehicle registration data. The use of biometrics and DNA registration has been touted as an efficient means of preventing and solving crime. Decade-long cases have been solved through registration and joint mobilization of police and judicial resources. The Prüm Treaty requires contracting parties to set up DNA profile databases and wide-scale exchange of personal data, and cross-border policing.

Although this initiative started as a multilateral agreement, a small group of influential countries led by Germany has successfully twisted other EU countries into integrating the provisions of the agreement into the legislative framework of the European Union under the Third Pillar. The treaty has been incorporated into a Council Decision binding on all EU member states. While the treaty represents a progress in the field of cooperation against crime, the implications of this treaty are far reaching. It raises privacy and data protection issues which will affect all EU citizens, primarily due to the absence of common legally binding data protection standards. The aim of this paper is to discuss the political and legal ramification of this legislation.

2. Background

The Prüm Treaty is an agreement amongst seven Member States – Germany, Austria, Spain, France, Belgium, The Netherlands and Luxembourg (other States later joined such as Finland, Italy, Portugal, etc.) outside the EU framework and aimed at improving cooperation in fighting terrorism and serious cross-border crime. It was signed on 27 May 2005 in Prüm, a small town in the west German land of Rhenania Palatinate. The treaty is often referred as the Schengen III because the same original intergovernmental grouping of powerful countries that signed the Schengen agreement (Belgium, Netherlands, Luxembourg, France and Germany) initiated the Prüm Convention. Although it bears the mark of the Schengen integration process, it is not a part of the Schengen Treaty.

The objective of the contracting states is to create a network of national databases where signatories can gain automated access to each other's national databases containing DNA analysis files and dactyloscopic (fingerprint) files[2] in what is called a hit/no hit system. Police could also launch a query in the data system of a contracting partner to find out whether it contains data concerning a specific profile, and are automatically informed of the result within a matter of minutes. They can also request specific related personal data from the Member State administering the file and, where necessary, request further information through the mutual assistance procedures, including those adopted pursuant to Framework Decision 2006/960/JHA.[3] The initiative must be seen as an implementation of the principle of availability that has been presented in the Hague Program of 2004 as an innovative approach to the cross-border exchange of law enforcement information.

The Prüm Treaty provides that reference data will not contain any information directly identifying a person although, in some cases, member states will also share suspects' personal data. In addition, the signatory states have agreed upon the possibility of hot pursuit of suspects across borders without prior consent in order to avert imminent danger to individuals. The integration is planned to take place, at the latest, three years after the entry into force of the treaty – a period which will start after the national parliaments ratify the Treaty.

From the onset, the ultimate aim of the framers under the German Presidency is to transpose the wording of the Prüm Treaty into EU legislation. The initial push for stronger EU-wide security legislation came from Germany, which co-authored the original Prüm Treaty. Article 1 (4) of the Prüm Treaty states:

> *Within three years at most following entry into force of this Convention, on the basis of an assessment of experience of its implementation, an initiative shall be submitted, in consultation with or on a proposal from the European Commission, in compliance with the provisions of the Treaty on European Union and the Treaty establishing the European Community, with the aim of incorporating the provisions of this Convention into the legal framework of the European Union.*

On 15 January 2007, using its EU Council Presidency, Germany submitted a proposal to make the Treaty applicable to all the member states. The Germany Presidency put the proposal forward without an explanatory memorandum, an impact assessment, nor an estimate of the cost to Member States, or time for proper consultation with Member States and the European Parliament. The intention was clearly to ensure that the essential elements of the Treaty would be transposed into a new EU law without change since the Treaty has already been signed by seven (7) Member States. Four days later, the Council Secretariat had already published a Working Paper containing a first draft of a Council Decision incorporating the Convention into EU law. It was *fait accompli*.

On 15 February 2007, the Council agreed to integrate the parts of the Treaty relating to information exchange and police cooperation into the EU legal framework .The draft Council Decision was sent to the European Parliament (EP) on February 28. Although the latter does not have a co-decision power in the Third Pillar matters, Article 39 of the Treaty on European Union requires the Council to consult the Parliament, and to give it a minimum of three months to deliver

[2] Dactyloscopic data include ''fingerprint images, images of fingerprint latents, palm prints, palm print latents as well as templates of such images (minutiae), as far as they are stored and dealt within an automated database''. Para 2.10 Note from Council Secretariat *Administrative and technical implementing Agreement to the Prüm Convention* Council of the European Union 5473/07, Brussels, 22 January 2007.

[3] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union lays down rules whereby the Member States' law enforcement authorities may exchange existing information and intelligence expeditiously and effectively for the purpose of carrying out criminal investigations or criminal intelligence operations.

its Opinion. The German Presidency asked the EP to deliver its opinion on or before the 7th of June.

On 4 April 2007, the European Data Protection Supervisor (EDPS) Peter Hustinx issued an opinion *ex officio*, since no request for advice had been sent to the EDPS. Hustinx questioned its legal basis since the treaty was conceptualized and initiated outside of EU institutional bodies by a limited number of individual Member States and is to be incorporated into EU law within two years of its signing. He also expressed his concerns as to the impact of the treaty on liberty since the long awaited general framework on data protection is not yet in place and negotiations are leading to a limited scope of application and minimal harmonization. He was concerned that in view of the absence of a general framework guaranteeing that data protection is embedded in this large scale exchange, a high rate of false matches in DNA and fingerprint comparisons would affect both the rights of the citizens and the efficiency of law enforcement authorities. At the EU level, current legislation protecting privacy and personal data protection has little, if any, application at the Third Pillar level. The Data Protection Commissioner recommends that a general framework for data protection in the Third Pillar must first be passed before implementing the Treaty into a Council Decision.

On 24 April 2007, the EP Committee on Civil Liberties, Justice and Home Affairs headed by Rapporteur Fausto Correia issued its committee report. The members of the Parliament Committee supported the idea of applying the Prüm treaty to all Member States, but called on the Council to amend the text accordingly. As the initiative relates to the purpose of approximation of laws and regulations of the Member States, the Committee recommended that the appropriate instrument must be a Framework Decision under Article 34(2) (b) of the EU Treaty, rather than a decision pursuant to Article 34(2) (c). The crucial difference, as far as the European Parliament is concerned, between decisions pursuant to Article 34(2) (c) and framework decisions adopted under Article 34(2) (b), is that whereas Parliament is consulted on the decision or framework decision itself pursuant to Article 39(1) of the EU Treaty, Article 34(2) (c) empowers the Council subsequently to adopt implementing measures by a qualified majority without consulting Parliament.

The Report also suggested several amendments at raising the level of protection of personal data, particularly in the specific case of DNA data, and at establishing that the future framework decision on the protection of personal data will also have to apply to these provisions. In particular, the amendment sought to ensure full compliance with the citizens' fundamental rights to respect for their private life and communications and to the protection of their personal data as enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. It also recommended that monitoring measures must be established. Furthermore, the Members of the European Parliament (MEPs) introduced an amendment to ensure that data collected under this decision will not be transferred or made available to a third country or to any international organisation. A number of amendments were suggested to ensure that the supplying of data is not made automatically but only when necessary and proportionate, and based on particular circumstances that give reasons to believe that criminal offences will be committed. The rapporteur introduced and negotiated amendments aimed at transforming the decision into a framework decision (on the advice of the EP's Committee on Legal Affairs), at strengthening operational cooperation (possibility of pursuit across borders and police cooperation on request).

On 9 May 2007, the European Union Committee of the House of Lords (UK) published a report examining the proposals to incorporate the Prüm Treaty into EU law and criticised the German EU Presidency for its failure to allow any opportunity for full consideration of the initiative by all Member States. However, the British government ignored the reservations. Ignoring the reservations raised by the House of Lords, Britain signed the parallel binding decision that replicates Prüm.

On 7 June 2007, the European Parliament issued its opinion and expressed regrets as to the obligation imposed on the Parliament by the Council to express its opinion as a matter of urgency. This had been without adequate and appropriate time for Parliamentary review and in the absence of both the comprehensive impact assessment and an evaluation of the application of the Prüm Treaty to date. There was also a lack of an adequate framework decision for the protection of personal data in police and judicial cooperation, which it considered was necessary before any legislation could be adopted under the Third Pillar (European Parliament legislative resolution, 7 June 2007).

At the European Council of ministers of Justice and Home Affairs (JHA Council) in Luxembourg on 12 June, the EU Home Affairs' Ministers agreed to transpose substantial parts of the Treaty into the EU's legal framework, i.e. into *Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime* (also referred to as Prüm Decision) which is binding on the Member States. In forcing it through, the Germans ignored the views of the European Parliament and the concerns of the EU data protection chief. The draft Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime was identical to the Prüm Treaty except that it omitted the right for police forces in ''hot pursuit'' of suspects to cross-borders, and cooperation around such issues as air marshals and immigration. With this Council Decision, the Prüm Treaty (or a version of it) would become part of the *aquis communitaire*, passing from the Third Pillar to the first and, therefore, from a mere form of cooperation into Community Method.[4]

3. Substantive law

The *Draft Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (Prüm Decision)* is based on the essential parts of the Prüm Treaty with the exception of the provision relating to cross-border police intervention in the event of imminent danger (Article 48) and affirms the principle of availability – the

[4] The Commission makes a proposal to the Council and the Parliament, which, in consultation with other EU consultative bodies, proposes amendments and adopts it as an EU law.

concept that information that is available to one law enforcement authority in the EU should be available to others. The decision contains rules in the following areas:

- on the conditions and procedure for the automated transfer of DNA profiles, dactyloscopic data and certain national vehicle registration data,
- on the conditions for the supply of data in connection with major events with a cross-border dimension,
- on the conditions for the supply of information in order to prevent terrorist offences, and
- on the conditions and procedure for stepping up cross-border police cooperation through various measures.

Chapter 2 Section 1 (Articles 2–7) contains rules on the conditions and procedure for the automated transfer of DNA profiles. Member States shall open and keep national DNA analysis files for the investigation of criminal offences. Member States are required to ensure the availability of reference data from their national DNA analysis files to other Member States. The DNA reference data which are to be exchanged are composed of a DNA profile and the non-DNA specific data.

Reference data shall only include DNA profiles established from the non-coding part of DNA and a reference. Reference data must not contain any data from which the data subject can be directly identified. DNA databanks normally register a profile not under the name of a person. A ''DNA profile'' means a letter or a number code which represents a set of identification characteristics of the non-coding part of an analysed human DNA sample, i.e. the particular chemical form at the various DNA locations (loci). A non-DNA specific data comprise an identification code or number allowing, in case of a match, the Parties to retrieve personal data and/or other information in their databases, a Party code to indicate the national origin of the DNA profile, and a code to indicate the type of DNA profile as declared by the Parties.

For the investigation of criminal offences, Member States shall allow other Member States' national contact points access to the reference data in their DNA analysis files, with the power to conduct automated searches by comparing DNA profiles. Should an automated search show that the supplied DNA profile matches DNA profiles entered in the receiving Member State's searched file, the national contact point of the searching Member State will receive in an automated way the reference data with which a match has been found (Article 3).

For the investigation of criminal offences, the Member States shall, by mutual consent, via their national contact points, compare the DNA profiles of their unidentified DNA profiles with all DNA profiles from other national DNA analysis files' reference data. Should a Member State find that any DNA profiles supplied match any of those in its DNA analysis files, it has to supply the other Member State's national contact point with the reference data with which a match has been found without delay (Article 4). Should there be a match; additional information can then be requested, such as the identity of the person concerned.

In situations where there is no DNA profile available for a particular individual present within a requested Member State's territory, the requested Member State has to provide legal assistance by collecting and examining cellular material from that individual and by supplying the DNA profile obtained only if the following conditions are met:

- the requesting Member State produces an investigation warrant or statement issued by the competent authority;
- the requesting Member State specifies the purpose for which this is required; and
- if there is an ongoing investigation or criminal proceeding. (Article 7).

Section 2 (Articles 8–11) contains provisions regulating the exchange of dactyloscopic data, which are defined as fingerprint images, images of fingerprint latents, and palm prints. For the prevention and investigation of criminal offences, Member States shall allow other Member States' national contact points access to the reference data in the automated fingerprint identification systems which they have established for that purpose, with the power to conduct automated searches by comparing dactyloscopic data. Should the procedure show a match between the dactyloscopic data, additional information can be requested through the national contact point? Reference data shall only include dactyloscopic data and a reference number. Reference data shall not contain any data from which the data subject can be directly identified. Reference data which is not attributed to any individual (unidentified dactyloscopic data) must be recognizable as such (Article 8).

Chapter 2, Section 3 (Article 12) deals with the rights of the member states to access the vehicle databases for criminal prosecutions and for reasons of preventing dangers for public security and order, i.e. including supposed threats to public order. Online access will be carried out according to the law of the requesting state.

Chapter 3 (Articles 13–15) provides for the prevention of criminal offences and in maintaining public order and security for major events with a cross-border dimension, in particular for sporting events or European Council meetings. Member States, both upon request and their own accord and in compliance with the supplying Member State's national law, have to supply one another with any non-personal data required for those purposes. Personal data will also be provided if any final convictions or other circumstances give reason to believe that the data subjects will commit criminal offences at the events or pose a threat to public order and security. The data supplied can only be retained for a year.

Chapter 4 (Article 16) contains provisions concerning information exchange to prevent terrorist attacks. Member States may, even without being requested to do so, supply other Member States' national contact points with the personal data and information, such as surname, first names, date and place of birth and a description of the circumstances giving rise to believe that the data subjects will commit criminal offences as referred to in Articles 1–3 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism. However, this provision is limited by Article 16(4) which gives the transmitting authority the power to impose conditions on the use made of such data and information by the receiving Member State. The receiving Member State is bound by any such conditions.

Member States may also conduct joint patrols and other joint operations in which designated officers or other officials from other Member States participate in operations within a Member State's territory (Chapter 5). In connection with mass gatherings and similar major events, disasters and serious accidents, Member States' competent authorities are obliged to provide one another with mutual assistance by notifying one another as promptly as possible of such situations with a cross-border impact and exchanging any relevant information and as far as possible, dispatching officers, specialists and advisers and supplying equipment, at the request of the Member State within whose territory the situation has arisen.

Chapter 6 (Articles 24–32) contains general provisions on data protection. Each Member State is required to guarantee a level of protection of personal data in its national law at least equal to that resulting from the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data of 28 January 1981.

Member states must ensure that personal data are effectively protected against accidental or unauthorised destruction, accidental loss, unauthorised access, unauthorised or accidental alteration and unauthorised disclosure (Article 29). Automated search procedure must also guarantee the following (Article 30(2)):

(a) state-of-the-art technical measures are taken to ensure data protection and data security, in particular data confidentiality and integrity;
(b) encryption and authorisation procedures recognised by the competent authorities are used when having recourse to generally accessible networks; and
(c) the admissibility of searches in accordance with Articles 31(2), (4) and (5) can be checked.

Article 31 provides special rules governing non-automated supply and every non-automated receipt of personal data by the body administering the file.

Article 32 contains the data subjects' rights to obtain information upon production of proof of his identity, without unreasonable expense, in general comprehensible terms and without unacceptable delays. This information refers to the data processed in respect of his person, the origin of the data, the recipient or groups of recipients, the intended purpose of the processing and, where required by national law, the legal basis for the processing. Moreover, the data subject shall be entitled to have inaccurate data corrected and unlawfully processed data deleted. The Member States shall also ensure that, in the event of violation of his rights in relation to data protection, the data subject shall be able to lodge an effective complaint to an independent court or a tribunal within the meaning of Article 6(1) of the European Convention on Human Rights or an independent supervisory authority within the meaning of Article 28 of 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. The data subjects are also given the possibility to claim for damages or to seek another form of legal compensation. The detailed rules for the procedure to assert these rights and the reasons for limiting the right of access shall be governed by the relevant national legal provisions of the Member State where the data subject asserts his rights.

4. German hegemony

4.1. *Democratic deficiency*

Legislative action within the EU has its problems. The proposed decision has been decried by numerous sectors as ''undemocratic''. The Council Decision bypassed the democratic process by being based on a treaty signed by only seven nations, and passed in the EU's Council of Ministers with little debate. Because it is an initiative of a Member State rather than a Commission proposal, there is no obligation to include an explanatory memorandum, a regulatory impact assessment or a cost estimate, and none are included.

All Community acts must be founded upon a legal basis as laid down in the Treaty (or in another legal act which they are intended to implement). The legal basis defines the Community's competence *ratione materiae* and specifies how that competence is to be exercised, namely the legislative instrument(s) which may be used and the decision-making procedure. The Council ignored the European Parliament's recommendation that the draft legislation must be a Framework Decision under Article 34(2) (b) of the EU Treaty, rather than a Decision pursuant to Article 34(2) (c).

The Parliament Committee on Legal Affairs stressed that it is clear from settled case-law of the Court of Justice (Case C-300/89, *Commission* v. *Council* [1991] ECR I-287, para. 10, and Case C-42/97, *European Parliament* v. *Council* [1999] ECR I-869, para. 36) that the choice of legal basis is not at the discretion of the Community legislator but must be determined by objective factors which can be subject to judicial review, such as the aim and content of the measure in question. In Case C-105/03 *Pupino*, the Court of Justice made it clear in its judgment of 16 June 2005 in that ''the wording'' of Article 34(2) (b) EU is very closely inspired by that of the third paragraph of Article 249 EC. Article 34(2) (b) EU confers a binding character on framework decisions in the sense that they 'bind' the Member States 'as to the result to be achieved but shall leave to the national authorities the choice of form and methods'. Consequently, a framework decision is the equivalent of a First Pillar directive, but without direct effect (Parliamentary Report, 2007).

The Committee also stressed that since ''decisions'' within the meaning of Article 34(2) (c) expressly exclude any approximation of national laws and regulations, it goes without saying that if the initiative under consideration involves any such approximation, it (the initiative) should take the form of a framework decision pursuant to Article 34(2) (b) instead.

4.2. *Pertinent provisions of the EU Treaty*

Article 34

2. The Council shall take measures and promote cooperation, using the appropriate form and procedures as set

out in this title, contributing to the pursuit of the objectives of the Union. To that end, acting unanimously on the initiative of any Member State or of the Commission, the Council may:

(b) adopt framework decisions for the purpose of approximation of the laws and regulations of the Member States. Framework decisions shall be binding upon the Member States as to the result to be achieved but shall leave to the national authorities the choice of form and methods. They shall not entail direct effect;

(c) adopt decisions for any other purpose consistent with the objectives of this title, excluding any approximation of the laws and regulations of the Member States. These decisions shall be binding and shall not entail direct effect; the Council, acting by a qualified majority, shall adopt measures necessary to implement those decisions at the level of the Union;

The choice for basing the Prüm rules on a ''decision'' and not a ''framework decision'' is based on the possibility to implement ''decisions'' by qualified majority (Article 34(2) (c) EU Treaty); for ''framework decisions'' this option does not exist. In this way, qualified majority voting could be introduced into matters of the Third Pillar. The draft Council Decision initiative takes existing mechanisms – procedures for access rights to automated DNA files, automated dactyloscopic identification systems and vehicle registration data – and, in certain circumstances, subject to specified conditions, affords them cross-border effect, which, as is abundantly clear from an analysis of the text, requires approximation of the relevant national rules. Moreover, the text as it is currently being considered by the Council contains a substantial chapter on data protection, which can also be regarded as constituting an approximation of national laws and regulations. Thus, the Committee on legal Affairs further stressed that the initiative for a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, should take the form of a framework decision and be based on Article 34(2) (b) of the EU Treaty and not the form of a decision based on Article 34(2) (c).

Nevertheless, the Council ignored the democratic control of the European Parliament and further weakened the parliament, which is already suffering for its failure to exist as a natural conduit connecting citizens to the European Union (Few Europeans know who their MEP is and what they do all day!).

The (UK) House of Lords European Union Committee also assailed the undemocratic process by which the Prüm Treaty was forced upon other Member States. On 9 May 2007, the (UK) House of Lords European Union Committee published the report Prüm: an effective weapon against terrorism and crime? (18th Report, Session 2006–07, HL Paper 90) examining the proposals to incorporate the Prüm Treaty into EU law and criticising the German EU Presidency for its failure to allow any opportunity for full consideration of the initiative by all Member States. The Committee criticised that the draft Council Decision was an initiative of a few member states. The Council Decision extended the application of the Treaty of Prüm, concluded between seven member states, to the whole EU without allowing for any major revision. As such, the other member states that are not involved from the beginning in the negotiation have no chance to shape the choice of rules. Their only choice is to either take-it or leave-it.

The European Data Protection Supervisor also criticised the legislative shortcuts through the EU's complex procedures that the German Presidency took. The UK House of Lords commented: ''The EDPS has said that parties to the Prüm Treaty have evaded the substantive and procedural requirements of enhanced cooperation'' and that it is arguable that ''the Prüm Convention breaches the law of the European Union'' (House of Lords, 2007).

It must be pointed out that an initiative of this significance was adopted on a multilateral intergovernmental basis, with a hard core of countries negotiating and signing up to an initiative and leaving the door open for other countries to join later, rather than developing this process through EU channels. This may be a way for Germany and its cohorts to push the Treaty through the back door to avoid substantive debate and possible public protest.

EU Commissioner Franco Fratinni has thrown his weight behind the German initiative. Speaking before the parliament's civil liberties committee, he declared:

> *You either accept Prüm [Treaty] or we [the European Commission] have to make a proposal for enhanced cooperation (Eurofacts, 2007).*

In spite of the Commissioner's threat, the fact remains that the German Presidency bypassed the Commission as the representative of community interest. Had the Draft Decision been a Commission initiative, it would contain an explanatory memorandum and assessment of cost for consideration. (Due to the haste of the German presidency to force its initiative on EU citizens, it failed to produce the necessary impact assessment and explanatory memorandum.)

British officials also expressed several reservations about the plan, in spite of the assurances of the German Interior Minister Wolfgang Schäuble that it had cost Berlin only €930,000, or $1.2 million, to create such a database (Dempsey, 2007). The amount is not reassuring given the fact that no actual cost estimates, even for internal purposes, have ever been made by the Member States.

The cost is not the real issue. The fundamental point is that community policies, which affect the rights of EU citizens must be transparent, open to scrutiny and accountable to the citizens and their representatives.

4.3. *Innocent 'lambs for slaughter'*

The National DNA database is a key police intelligence tool which contributes to the efficiency of crime detection. It has a key role to play in contributing to detection outcomes, eliminating the innocent from inquiries, focusing the direction of inquiries resulting in savings in police time and in building public confidence that elusive offenders may be detected and brought to justice.

In pushing for an EU legislation on an EU-wide access to DNA and fingerprint database, Germany cites the success of the cross-border exchange of DNA and fingerprint data

between Germany and Austria which began in December 2006. It claims that matching the profiles has resulted in thousands of hits and Germany reports that the matching of untraceables between German and Austrian databases is impressive. The beneficial results of the Prüm treaty are already evident, stated Minister Schauble:

> *There have been more than 1500 hits when Austrian data were matched against data held in Germany, and vice versa over 1400 hits were produced when German data were matched against data held in Austrian databases. 32 hits alone were produced with regard to manslaughter or murder cases. Let me give you an example: A sexual offender brutally raped two women in the German town Gelsenkirchen in 2003 and 2004. No leads whatsoever were found. As these data were matched against data held in Austria, it was possible to establish the identity of the alleged perpetrator, who is from the German town Halle on the Saale, because he had also raped a woman in Austria and was temporarily detained there. It is true that unsolved cases cannot be finally settled by means of the hits produced in the Prüm matching processes. Further steps need to be taken to produce hard evidence and solve the case in hand. This is why at present, just two months after we started data matching, we cannot produce any final investigative results or present cases we have been able to settle. However, the intelligence produced in the matching processes open up fresh and promising leads, and help the criminal prosecution authorities in their daily investigative work* (Magazin, 2007).

In a further statement, Germany claims:

> *Under the treaty Austria and Germany have been able to check the contents of their national DNA databases against each other since early December 2006. This is the first time that two countries have granted each other access to their national police databases using a hit/no hit method. In just six weeks, when German untraceables were checked against the Austrian database, 1500 matches were found, and when Austrian untraceables were checked against the German database, 1400 matches resulted. "On the basis of these results, where untraceables could be matched with a person in the database, police investigators are now able to match hits with unsolved crimes. Thus, it can be expected that Germany and Austria will be able to solve unsolved crimes and prosecute and punish the offenders. These figures are proof that the idea behind the Prüm Treaty to create a network of existing national databases is a simple, yet very effective means to fight cross-border crime and international terrorism"* (Dempsey, 2007).

While the German report is impressive, the German–Austrian experiments have not been put into practice in a wider scale. The European Data Protection Supervisor is not convinced that the first results of this limited exchange only with two Member States involved can be used as giving sufficient empirical basis for making the system applicable to all the Member States. First, Germany and Austria share cultural and linguistic similarities, as well as geographical proximity. This approach is clearly inapplicable for countries with very different legal traditions. Second, there is no standard EU policy for the collection and retention of the sorts of data that the Decision (Prüm) deals in. MEP Philip Bradbourn, Conservative Spokesman on Justice and Home Affairs, commented (Conservatives, 2007):

> *This Treaty fundamentally goes against the rules of data protection and civil liberties that we have come to expect in Europe. This "one size fits all" approach is clearly inapplicable for countries with very different legal traditions and even senior police in the UK have called for this Treaty to be scrapped, proposing that voluntary bilateral agreements between Member States should be the way forward in security cooperation.*

The British have legitimate reasons to worry. The most developed database in Europe (and in the world) is the DNA database in the United Kingdom. Set up in 1995 by the Forensic Science Service (FSS), the national DNA Database (NDNAD) of England and Wales is the largest in the world. At the end of January 2007, it contained over 3.8 million profiles. The NDNAD dwarfs other genetic databases in countries with similar populations (such as Germany) and those with significantly larger populations (such as the US). It is the largest database of its kind worldwide in both relative terms and absolute terms (Application nos. 30562/04 30566/04 in the European Court of Human Rights, 2007). Laws currently allow samples to be taken from anyone suspected of, charged with, reported for or convicted of a recordable offence. At present, DNA samples (intimate or non-intimate) can be obtained from

- anyone arrested/detained for a recordable offence and
- volunteers (with *irrevocable* consent).

The NDNAD is unique because it is the only national DNA database in the world, which retains the biological information and DNA profiles of individuals on a permanent basis. These individuals may have never been charged or convicted of an offence. No other countries adopt this system. The situation is different in other countries. For instance, in Germany profiles are only held for those who have been convicted of serious offences.

England and Wales also have the largest fingerprint database (NAFIS) in the world, in relative terms. They are unusual because the law allows them to retain fingerprint information even after acquittal or the dropping of charges against a suspect. In most other countries, it is routine for those prints to be destroyed if the individual is not subsequently convicted of a crime. Thus, the current system of safeguards, given the privacy implications of the information contained in samples and profiles, is inadequate in the UK.

The implication for innocent people is worrying. According to David Davis, the Shadow Home Secretary,

> *The government's track record with IT and database projects is woeful. Take the Home Office. The criminal records bureau wrongly labelled 2700 innocent people as having criminal records. The sex offenders' register lost more than 300 serious criminals. And the convictions of 27,000 criminals – including murderers, rapists and paedophiles – were left off the police national computer. Finally, the DNA database combines the worst of all worlds: 100,000 innocent children who should never have been on it, 26,000 police-collected samples left off it and half*

a million entries misrecorded (Application nos. 30562/04 30566/04 in the European Court of Human Rights, 2007).

The misgivings come down to the citizen's mistrust of the government and the people's fears of an Orwellian future. It has just been revealed that there are 550,000 false misspelt or incorrect names on the existing (UK) database and there are fears that the bumbling government cannot be entrusted to keep the data secure. There are also legitimate worries that government could use the DNA records to track down innocent movements, come up with unknown uses and applications for the DNA, or even sell the DNA profiles to insurance companies at some future date.

Now that the British government has given its assent to the Prüm Decision, the NDNAD will be open to further cross-border access. Other member states will have access to samples and profiles of innocent persons who have been profiled in the databases. The Draft Decision unfortunately fails to specify the categories of persons that will be included in the databases. Different Member States have different reasons for collecting DNA or different thresholds at which they keep people's DNA and dactyloscopic files. Many fear that the officials of a country which holds DNA data only for serious crimes will inevitably start with the presumption that DNA data are held in the United Kingdom for the same purpose, and perhaps put at risk those whose DNA is held because they have committed only a minor crime, or perhaps no crime at all.

In probably one of the most important human rights cases of all time, two British men asked the European Court of Human Rights on 27 February 2008 to have their DNA removed from the national database. Mr. Michael Marper was arrested in 2001 when his former partner accused him of harassment. The charges were dropped, but the police refused to destroy his DNA profile. The other case involves a 19 year old man, referred only as ''S'', who was arrested in the same year when he was only 11, but later acquitted of all charges in court. For six years, the two men have fought their case all the way to the House of Lords who upheld the government's DNA data retention policy. The two men then complained to the ECHR, who will now decide whether the current system of retaining innocent Britons DNA permanently on the database breaches the rights to privacy. The outcome of the appeal could lead to the destruction of the DNA and fingerprint evidence of people that have been found innocent and could torpedo the proposal of Lord Justice Stephen Sedley to put everyone in the UK, including visitors who stay for only one week, on a DNA database.

The German Presidency's enthusiasm for the results achieved by matching DNA profiles held in its database with those held by the Austrians ignores other problems which are likely to arise when the same exercise is carried out among 27 Member States. The DNA bases are also characterized by high error rates, due to both fault rates intrinsic to the used technologies and to the lack of police database updates, inter alia in accordance with judicial outcomes of the recorded cases. Sharing such files among 27 countries would certainly increase not only massive surveillance but also the risk of flaws endangering innocents (Davis, 2007).

The absence of a harmonised approach to the collection and retention of data means, for instance, that there will continue to be differences between the grounds on which Member States collect DNA and fingerprints, and the length of time they are allowed to retain these data under their national law (e-gov Monitor, 2007). The sensitive personal data of innocent people should not be shared around Europe.

4.4. *Data protection*

The draft Council Prüm Decision is mainly concerned with the exchange of data. Inevitably this raises data protection issues. As such, the European Data Protection Supervisor should be entitled to have a say in the classes of information which are to be exchanged, the procedures for exchanging them and the safeguards which will apply. However, the Council did not bother to seek the opinion of the European Data Protection Supervisor, even though under Article 41 of Regulation (EC) No. 45/2001, the European Data Protection Supervisor is responsible for advising on this initiative since this falls within the limits of the task entrusted to him.

The European Data Protection Supervisor issued a detailed opinion on the Prüm Decision. Although he is not opposed to the idea of cooperation between member states in fighting terrorism, he proposed some amendments to strengthen data protection and privacy. While it is his opinion that the draft Council Decision offers in substance an appropriate protection, he nevertheless opposed it since it will rely on local and possibly inconsistent data protection laws. There is presently no general rule on data protection in the Third Pillar. The current Data Protection Directive is only binding on the First Pillar.

Although the proposed Council Decision refers to the *Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* of 28 January 1981 and its *Additional Protocol* of 8 November 2001, it is not precise nor is it binding on the EU Member States. He emphasized that the Prüm Decision should build on a general framework of data protection in the Third Pillar, and should not be adopted before the adoption of a framework on data protection guaranteeing an appropriate level of data protection. Currently, a Data Protection Framework has been proposed but has not been adopted. Without the Framework Decision on Data Protection in place, the proposed draft Prüm Decision would not provide sufficient data protection safeguards. The harmonization of data protection laws under the Third Pillar would harmonise the national laws. A legal framework for data protection is a *condicio sine qua non* for the exchange of personal data by law enforcement authorities, as is required by Article 30 (1) (b) of the EU Treaty, and recognised in several EU policy documents (Opinion of the Data Protection Supervisor, 2007).

The Data Protection Supervisor further stated:

> *The initiative relies on the presupposition that matching DNA profiles is the key instrument in police cooperation. For this reason, all Member States have to establish DNA databases for the purposes of criminal justice. Taking into account the costs of these databases and the risks from the perspective of data protection, a thorough ex ante assessment is needed of the effectiveness of this instrument (Opinion of the Data Protection Supervisor, 2007*).

The Justice Committee of the UK House of Commons has just issued on 3 January 2008 a report on public data protection since the Chancellor announced to Parliament in November last year that HMRC had lost confidential records affecting 25 million UK citizens. The report expresses Parliament's apprehension about the risks associated with big databases containing personal data that are open to large numbers of licensed users, as well as the obligation to share the data under the Prüm Decision. The House of Commons Justice report (2008) stated:

> *Linked to issues of adequacy of data protection in the UK is the matter of data exchange and protection at EU level in the context of greater interoperability of Government databases, which the UK Government and those of other EU member states aspire to. The EU Framework Decisions incorporating the Prüm Treaty into EU law and establishing the 'principle of availability' of Government-held information between EU member state authorities will have a direct impact on the protection of data of UK citizens held by the UK Government. If data held by the Government is available for inspection outside the jurisdiction, then the importance of restricting the amount of data held, as well as proper policing of who had access to it, takes on even greater importance.*

The report also recommends that personal data should be held only where there are proper safeguards for the protection of the respective data, which, in the Justice Committee's opinion will become ever more difficult as data can be easily shared within the country as well as between countries.

The Parliament is considering amending section 60 of the Data Protection Act through the Criminal Justice and Immigration Bill and imposing custodial sanction as well as the existing fines for those found guilty of unlawfully obtaining or disclosing personal data (Beith, 2008).

5. Conclusion

It is important that law enforcement authorities in the European Union should have the tools available to obtain information held by other EU countries as quickly as possible to help with the investigation and prevention of crime. While there is indeed a legitimate reason to exploit the full potential of databases to combat terrorism and combat crime, it should not be used as a rationale for adopting such measures behind hidden doors and bereft of a national debate. What is appalling is the way a few Member States led by the German Presidency have made agreements, with limited or inadequate protections for the citizens, amongst them and then forces it on other Member States.

While it is normal for the Germans to use the Presidency to promote legislative proposals, it should not be a reason for cutting short full consideration of the Member States, sidelining the European Data Protection Supervisor's opinion and ignoring the views of the European Parliament.

What brings most to the truly atrocious aspect of all this is the lack of democratic control and protection of data privacy. The German presidency – with not even a pang of conscience – has felt free to increase its investigative and police hegemony over the other Member States. This is the kind of lapse that wills the nations' collapse. It is just sheer tastelessness. It is just sheer greediness. It is pure arrogance.

The attempt to subvert legitimate resistance in the other countries, through reaching a special agreement with some of the member states, is being described in the German press as a novelty in the European integration process. It is being voiced, that this is opening the possibility of enforcing numerous legal norms, in spite of their far reaching consequences, without ratification by the entire EU (European Achievement, 2007).

This is a dangerous precedent. Privacy has become subservient to security.

Sylvia Kierkegaard, *sylvia@kierkegaard.co.uk, Report Correspondent, President, International Association of IT Lawyers.*

REFERENCES

Application nos. 30562/04 30566/04 in the European Court of Human Rights. <http://www.poptel.org.uk/statewatch/news/2007/nov/echr-marper-submissions-15-03-07-final.pdf>; 15 March 2007 [retrieved 27.01.2008].

Beith A. Tougher data laws needed, say MPs – BBC News. <http://news.bbc.co.uk/1/hi/uk_politics/7168588.stm>; 3 January 2008 [retrieved 28.01.2008].

Conservatives. EU Constitution moves in by the back door, <http://www.conservatives.com/tile.do?def=wales.news.story.page&obj_id=137043>; 7 June 2007 [retrieved 27.01.2008].

Davis D. Beware the state's ID card sharks – Sunday Times Online, <http://www.timesonline.co.uk/tol/comment/columnists/guest_contributors/article3108069.ece>; 30 December 2007 [retrieved 27.01.2008].

Dempsey J. Germany seeks to modernize policing across EU. International Herald Tribune, <http://www.iht.com/articles/2007/01/15/news/germany.php>; 15 June 2007 [retrieved 26.01.2007].

Eurofacts. Slimmed down treaty: the greatest threat to UK, <http://www.junepress.com/PDF/Vol%2012%20No%20%209%20-%209th%20February%202007.pdf>; 9 February 2007 [retrieved 27.01.2008].

European Achievement. German-Foreign-Policy.com, <http://ftrsupplemental.blogspot.com/2007/01/european-achievement.html>; 17 January 2007.

European Parliament legislative resolution on the initiative by the Kingdom of Belgium, the Republic of Bulgaria, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Republic of Austria, the Republic of Slovenia, the Slovak Republic, the Italian Republic, the Republic of Finland, the Portuguese Republic, Romania and the Kingdom of Sweden on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (6566/2007 – C6-0079/2007 – 2007/0804(CNS)), <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P6-TA-2007-0228>; 7 June 2007 [retrieved 27.01.2008].

e-gov Monitor. Home affairs ministers back initiative to create a pan-European network of police databases for more effective crime control, <http://www.egovmonitor.com/node/9093>; 18 January 2007 [retrieved 27.01.2008].

House of Commons Justice report. House of commons, <http://www.publications.parliament.uk/pa/cm200708/cmselect/cmjust/154/15402.htm>; 2008 [retrieved 28.01.2008].

House of Lords. Prüm: an effective weapon against terrorism and crime? Statewatch, <http://www.statewatch.org/news/2007/may/eu-hol-prum-report.pdf>; 9 May 2007 [retrieved 27.06.2008].

Magazin DBB. The Treaty of Prüm makes Europe safer – EU police forces share data, <http://www.bmi.bund.de/cln_012/nn_942674/Internet/Content/Nachrichten/Medienspiegel/2007/03/Hanning__dbb__en.html>; March 2007 [retrieved 27.01.2008].

Opinion of the European Data Protection Supervisor on the Initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Republic of Austria, the Republic of Slovenia, the Slovak Republic, the Italian Republic, the Republic of Finland, the Portuguese Republic, Romania and the Kingdom of Sweden, with a view to adopting a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (2007/C 169/02), <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-04-04_crossborder_cooperation_EN.pdf>; 2007.

Parliamentary Report on the initiative by the Kingdom of Belgium, the Republic of Bulgaria, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Republic of Austria, the Republic of Slovenia, the Slovak Republic, the Italian Republic, the Republic of Finland, the Portuguese Republic, Romania and the Kingdom of Sweden on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (6566/2007 – C6-0079/2007 – 2007/0804(CNS)), <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A6-2007-0207&language=EN#_part2_def1_part2_def1>; 24 May 2007 [retrieved 27.01.2008].