Note: This is the accepted version of the article. The published version can be found at the European Journal of Criminal Policy and Research DOI 10.1007/s10610-017-9355-0

Strengthening Cross-border Law Enforcement Cooperation in the EU: the Prüm Network of Data Exchange

Dr Oriola Sallavaci
Anglia Ruskin University
United Kingdom
Oriola.Sallavaci@anglia.ac.uk

Abstract

The Prüm network was established to provide mechanisms and the infrastructure to achieve a closer cooperation between the EU member states in combating terrorism, organised crime and illegal immigration through the cross border exchange of DNA profiles, fingerprints and vehicle registration data. While Prüm offers clear benefits for cross-border policing, it continues to present challenges of a technical and scientific nature as well as legal, ethical and socioeconomic concerns. This article reviews these challenges as well as the existing safeguards. It argues that, in order to achieve Prüm benefits and maximise its potential, it is important to enhance the necessary dialogue and cooperation between member states so as to confront the above concerns and address challenges posed by Prüm through balanced measures.

Keywords

Cross border crime; cross border data exchange; EU criminal justice; Prüm network; transnational policing; DNA; Fingerprints; Vehicle registration data

Acknowledgements

The author is grateful to the reviewers for their comments. The author would like to thank Harry Haycraft for his assistance with this research.

Funding

This work is partly based on research funded by Anglia Ruskin University.

Conflict of Interest

The author declares no conflict of interest

Introduction

During the past decades, the EU member states have increased their efforts in the fight against terrorism, organized crime and illegal immigration. Increasingly, terrorism and other serious crime have developed a cross border dimension, which is accentuated by the dismantling of internal border controls within the Schengen free movement area and ease of travel and communication within the EU and beyond. Recent terrorist attacks in Europe have demonstrated that the need for closer transnational cooperation to prevent atrocities and to achieve a swift and efficient law enforcement response is paramount. In the wider context of transnational cooperation, information exchanges between law enforcement authorities are essential in fighting cross border crime and to ensure a high level of security in the EU.

In order to achieve timely access to accurate and up-to-date data for law enforcement authorities, a number of EU instruments and systems have been put in place in recent years, supplemented by international and bilateral arrangements. These instruments fall within overarching objectives set by the Lisbon Treaty (Art 87 TFEU); specific principles and policy frameworks set out in the Hague 2005 and Stockholm 2010 Programmes - including *availability* and *mutual recognition*; Council's Information Management Strategy 2009 and the related Action Plans; Commission Communications and studies (COM(2010)385) and have to be applied with respect for fundamental rights (Art 6 TEU).

The key instruments for law enforcement information exchange in the EU include: the *Swedish Framework Decision* (Council Framework Decision 2006/960 JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union) which covers the exchange of information for the purpose of criminal investigations or criminal intelligence operations, with a particular focus on access to information; the *Prüm Decisions* (Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime and Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation particularly in combating terrorism and cross-border crime) which provide for automated exchange of biometric data (DNA profiles and fingerprint data) and vehicle registration data for the prevention and investigation of criminal offences and maintaining public security; Council Decision 2007/533/JHA on the establishment, operation and use of the *second generation Schengen Information System* (SIS II) which provides alerts on persons and objects, and Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (*Europol*), which provides inter alia for the collection, storage, processing, analysis, and exchange of information and intelligence.

This article focuses on the cross border exchange of bio-information specifically of DNA and fingerprints. Given the importance and the nature of information that DNA and fingerprints in particular offer for investigations and prosecutions in a domestic level, their cross border exchange acquires great relevance as an unparalleled facilitating tool of transnational policing cooperation. In Europe, traditional channels of cross border exchange of bio-information include *individual legal assistance requests* which, depending on the provisions of the domestic legislation in the respective countries, engage either police or judicial channels. Another important mechanism is *Interpol* through its established central databases of DNA and fingerprints. The DNA database is autonomous and does not keep any nominal data linking a DNA profile to any individual. The data is provided by its member states which in turn use them for comparison. Member states retain the ownership of their profile data and control its submission, access by other countries and destruction in accordance with their national laws. Where a match is found a message is sent to the countries contributing to the match. This message contains the basic case information that was provided and can optionally provide the sample codes. Member states then decide if they wish to pursue this forensic intelligence link (ENFSI 2016).

A great disadvantage of the traditional channels of information exchange is that they employ time consuming, complex bureaucratic procedures, which are counterproductive in criminal investigations (ENFSI 2016). One of the most recent and significant measures to facilitate the cross border exchange of bio-information has been the network established in 2005 by the Treaty of Prüm (originally signed by the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain; the French Republic; the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria). The Prüm network was transformed into EU –wide cooperation tool through the Council Decision 2008/615/ JHA and Council Decision 2008/616/JHA becoming *acquis communaitaire* binding on all existing and new EU member states. The ultimate goal of the Prüm network is to overcome the lengthy mutual legal assistance bureaucratic procedures by establishing a single national contact point as an electronic interface for automated information exchange. Traditional channels of legal assistance are only activated when search data matches a stored entry whereby a hit would lead to a request for further information (Topfer 2011).

The Prüm network provides for the exchange of DNA profiles (in 15 minutes), fingerprints (in 24 hours) and vehicle registration data (in 10 seconds) across all the EU Member States which have not opted out of the measures (Home Office 2015). Prüm Decisions may be used for the exchange of personal data regarding the prevention of terrorist offences and joint operations by police agencies of Member States. While Prüm offers clear benefits for cross-border policing, it continues to present challenges of a technical and scientific nature as well as legal, ethical and socioeconomic concerns. This paper reviews these challenges as well as the existing safeguards. It argues that, in the name of benefits that Prüm offers and in order to maximise its potential, it is important to enhance the necessary dialogue and cooperation between member states so as to confront the above concerns and address challenges posed by Prüm through balanced measures.

Prüm network of cross border information exchange: a brief overview

The Prüm regime of cross border information exchange is based on three measures: Council Decision 2008/615/JHA on the stepping up of cross border cooperation, particularly in combating terrorism and cross border crime; Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA and Council Framework Decision 2009/905/JHA on accreditation of forensic service providers carrying out laboratory activities. The first two measures, referred to as *Prüm decisions*, have the following main elements:

- Chapter 2 of the Council Decision 2008/615/JHA and Chapters 2-6 of the Council Decision 2008/616/JHA provide for the automated search and comparison of data from national data files in the area of DNA, dactyloscopic [fingerprint] data and vehicle registration data.
- Chapters 3 and 4 of the Council Decision 2008/615/JHA deal specifically with information exchange for the prevention of offences in the context of major events with a cross-border dimension (such as sporting events or European Council meetings) and measures to prevent terrorist offences.
- Chapter 5 of the Council Decision 2008/615/JHA and Chapter 6 of the Council Decision 2008/616/JHA provide for other forms of law enforcement cooperation including joint operations and mutual assistance in connection with mass gatherings disasters and serious accidents.
- The operational chapters are underpinned by Data Protection rules set out in Chapter 6 of Council Decision 2008/615/JHA.

Under the terms of the Prüm decisions, contracting states have reciprocal access to national databases containing DNA profiles, fingerprints and vehicle registration data and are allowed to conduct searches in an automated way through their nominated contact points holding authorisation to carry out automated searches (Council Decision 2008/615/JHA - Article 2). DNA profiles, fingerprints and vehicle registration must be in relation to an identifiable individual or to a criminal incident. Prüm operates as a hit/no hit system similar to that used by Interpol discussed above. The initial automated search of national databases excludes personal data with the exchange of such personal information occurring at a later stage. After a hit or a match, countries can obtain the personal and/or case information associated with the DNA-profile or fingerprint via existing mutual legal assistance procedures, through police or judicial channels. A request for personal data is regulated by the national legislation of the requested Member State. While the reported low volume of transactions through Interpol may be attributed to "often poorly defined and cumbersome" processes, as well as unpredictable response times, Prüm offers a more efficient process, either wholly (for vehicle registration data) or partially (for DNA profiles and fingerprints) automated and subject to strict response times which make Prüm a much more useful operational tool for the police working on real time investigations (House of Commons 2015).

To enable the automatic exchange, each country creates a copy of its DNA-database with a standardized table structure, which can be accessed by common data exchange and DNA

comparison software present in each country (Council Decision 2008/615/JHA). The requirement for a *copy* DNA database allows member states to apply filters that limit the scope and category of profiles and data being fed to the Prüm network; for instance a country may decide not to upload profiles obtained by a certain category of individuals such as victims or volunteers. Prüm decisions do not contain any requirements as to the scope of profiles and information to be included in each national database and therefore which profiles or data will need be exchanged; whether or not DNA samples should be retained and after what amount of time samples, profiles and fingerprints should be deleted from the system.

It has been questioned whether the Prüm regime sufficiently upholds the principle of *availability* introduced by the Hague Programme 2005 according to which information for law enforcement purposes needed by authorities of one Member State are to be made available by the authorities of the Member State where the information is stored. According to the principle of availability, there should be as few obstacles as possible in the way of an official from one Member State accessing information held by another Member State. Combined with the principle of *mutual recognition* which holds that information collected or produced by one Member State should be deemed as valid as that collected or produced by another, disparate Member States become part of the single entity: the Area of Freedom Security and Justice (Jones 2012). It has been argued that under Prüm, data does not become constitutive of a common area wherein national sovereignty on data is relaxed; less data will be exchanged under Prüm than foreseen under the principle of availability as indirect access to data is the norm (Bellanova 2008).

While the principle of availability is arguably a vision worth pursuing, in practice, at least for the time being, it can work only partially. It is impossible to realise its full potential as long as there still exist different national, legal and administrative systems, data protection legislations and interoperability problems (Jones 2012) It is impossible for the aspirations highlighted by the above principles to be achieved without the standardisation of the technology and procedure as well as the harmonisation of respective domestic legal instruments. Cross border exchange of information raises particular ethical and legal concerns as sensitive personal data such as DNA and fingerprints obtained and retained in one country leave the jurisdiction and legal protection afforded by the legal framework of that country. There is a need to strike the right balance between the public interest in fighting crime which requires information exchange and the protection of the rights involved; consequently safeguards and limitations are necessary.

The European Council stressed that the following conditions should be observed in the implementation of the principle of availability (Hague Programme 2005):

- The exchange may only take place in order for legal tasks to be performed;
- The integrity of the data to be exchanged must be guaranteed;
- The need to protect sources of information and secure the confidentiality of the data at all stages of the exchange, and subsequently;
- Common standards for access to the data and common technical standards must be applied;

- Supervision of respect for data protection, and appropriate control prior to and after the exchange must be ensured; and
- Individuals must be protected from abuse of data and have the right to seek correction of incorrect data.

To this end, Prüm sets out a number of data protection safeguards. Article 25(1) of the Council Decision 2008/615/JHA requires Member States to guarantee a level of protection 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 (Convention 108) and its Additional Protocol of 8 November 2001. Article 25(2) states that a Member State may only exchange information if it has passed a data protection evaluation. Article 26 concerns purpose limitation. The processing of data by the receiving Member State shall be permitted solely for the purposes for which the data have been supplied defined as: (a) Establishing whether the compared DNA profiles or dactyloscopic data match; (b) Preparing and submitting a police or judicial request for legal assistance in compliance with national law if those data match; and (c) Recording within the meaning of Article 30. Data supplied must be deleted unless it is required for the purposes set out in points (b) and (c) above, which means that profiles, fingerprints and license plate number/VINs cannot be stored on the receiving country's systems.

Article 28 sets out accuracy, current relevance and storage time of data requirements. This includes a requirement to notify a Member State if data supplied is incorrect or should not have been supplied. Any incorrect data should be corrected. If the accuracy or inaccuracy of data cannot be ascertained, the data are to be flagged. Member States cannot store data for longer than the law of the sending Member State permits. Article 29 requires Member States to have technical and organisational systems to ensure data is protected and kept securely. Article 30 sets out requirements for logging and recording, including what should be recorded, who should be authorised to access any data, and time limits for retention of the logging requirements. In Article 30(5), the Decision sets out that that the independent data protection authorities in each Member State should carry out random checks on the lawfulness of supply. Article 31 sets out data subject rights. Data must be supplied comprehensibly and without unacceptable delays, on 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 of data.

The data protection aspect of Prüm exchanges is not subject to the recent Directive 2016/680 on the protection of natural persons with regard to processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and on the free movement of such data repealing Council Framework Decision 2008/977/JHA. While a single, coherent data protection regime for all EU police and criminal justice measures may be attractive, it is difficult to be achieved in practice. The Prüm data protection rules deal specifically with data exchange within the scope of Prüm whereas the general rules within the new Data Protection Directive establish general principles that govern the exchange of data between and within Member States. Arguably it would be difficult to capture specific purpose limitation Prüm

requirements in a single set of general data protection rules applicable to all forms of cooperation in this field.

A further important aspect of the Prüm regime concerns the Council Framework Decision 2009/905/JHA on Accreditation of forensic service providers carrying out laboratory activities. The increasing cross border exchange of information and the use of forensic evidence from one member state to another highlights the need to establish common standards for forensic science providers. This is particularly important as information originated from forensic processes in one Member State may be associated with a level of uncertainty in another Member State regarding the way in which an item has been handled, what methods have been used and how the results have been interpreted (recital 4-5). The Framework Decision requires forensic service providers (for both fingerprints and DNA) to be accredited to ISO standard 17025. In compliance with the principle of *mutual recognition* it also requires Member States to treat forensic results from ISO 17025 accredited laboratories in Member States as they would a domestic ISO 17025 accredited laboratory (Article 1).

It can be seen that in its entirety the Prüm regime offers a number of safeguards to ensure adequate standards and the protection of individual rights related to the cross border exchange of personal data. As discussed above, each Member State may identify the data (DNA profiles, fingerprints etc.) accessible to other Member States and determine the conditions for automated searching (Council Decision 2008/616/JHA para 13 and 18). Moreover, automated searches may only be undertaken in individual crimes (Council Decision 2008/616/JHA article 3 para 1, article 9 para 1 and article 12 para 1). When a Member State joins the Prüm network they may undertake a large scale exchange of data against the complete Prüm databases however these safeguards provide data protection in relation to an individual's personal DNA profile, fingerprints and vehicle registration details conform requirements of necessity and proportionality (McCartney 2013). Member States will never obtain personal data about the DNA profiles/fingerprints that does not match the one submitted for the search, with personal data only being provided when a DNA profile/fingerprint receives a hit and the provisions of obtaining additional information about the purpose of the data are satisfied. Additionally, the appointed 'contact points' that can perform searches in the DNA/fingerprints databases of other countries must either be forensic services or law enforcement agencies responsible for information exchange (Soleto-Munoz and Fiodorova 2014).

These measures uphold the autonomy of Member States in determining which profiles/data are available and any conditions attached. Member States may curtail or advance the data provided, as much or as little as they see fit in line with their national law. As discussed further below, while on the one hand this aspect can be viewed as a safeguard, on the other hand the significant variation in terms of laws, regulations, and practices within the Prüm countries raises specific concerns in the context of cross border policing and personal data exchange (Prainsack and Toom 2013). To these challenges and concerns the attention now turns.

The ‘rocky path’ to implementation

One of the most prevalent criticisms of Prüm is that its implementation has not progressed smoothly or at the pace originally anticipated (Deloitte 2015). The Prüm Decisions should have been implemented fully by Member States by August 2011. At the time of writing, eight Member States had not yet completely implemented the Prüm Decisions, in particular with respect to the automated searches (Council 9823/16). 22 Member States have implemented the DNA data exchange, 18 Member States have implemented the fingerprint data category and 19 have implemented the vehicle registration data category (Commission 2015; Council 11001/16).

Becoming a member of the Prüm network is a complex political and technical process. There are multiple, time consuming requirements for complying with provisions on DNA profiles, fingerprints and vehicle registration data (Topfer 2011). The adjustment of domestic regulatory frameworks is required as well as the establishment of national contact points. The setup of central searchable databases connected to the secure European administrator intranet S-TESTA, the fulfilment of the minimum data protection requirements, the definition of search capacities and the implementation of technical specifications are but a few of the Prüm requirements. After every aspect is in place, several evaluation visits have to be hosted before the Council of Justice and Home Affairs Ministers (JHA) decides, unanimously, that a Member State is ready to start operational data exchange (Jones 2012).

Member states have faced difficulties in adjusting national legal frameworks with the Prüm requirements. There have been power struggles between agencies over the denomination of the national contact point, difficulties caused by intra-organisational restructuring required for transnational cooperation, technical challenges related to incompatibility of hardware/software components and connection issues, as well as scarcity in personnel and financial resources (Council 14918/10; Topfer 2011). Costs associated with Prüm implementation are considerable especially those to be borne by smaller states or those countries without established DNA databases (Deloitte 2015). The UK estimated that Prüm implementation would cost £13.5 million notwithstanding the UK’s already extensive DNA profile, fingerprints and vehicle registration databases (Home Office 2015). Other Member States have simply not been able to afford such costs and have continued to delay the implementation and operation of Prüm. A number of countries (such as Cyprus, Greece, Ireland, Italy, Malta, and Portugal) were still in the process of setting up their national DNA databases several years after the Prüm decisions (Prainsack and Toom 2013). Croatia and Italy were still planning how to implement Prüm by 2014 while Luxembourg had not even started plans for Prüm implementation by this time (Deloitte 2015).

While a Member State may be capable of exchanging information, the operability of the cross border exchange system is also dependant on the other Member States readiness to participate. As Prüm requires a decentralised network of national databases, over 30 bilateral interfaces are required. Most Member States start by connecting with one or two neighbouring countries, however as the costs for establishing connections are significant, they do not continue investing in creating connections with and extend their Prüm usage to all operational Member States (Deloitte 2015). It has been reported that Member States do not feel there is a binding obligation to interconnect completely. At the same time, partial implementation and Member States' reluctance affects their counterparts' abilities to expand their connections (Deloitte 2015). There are therefore real risks of relatively one-sided cooperation compared with the potential benefits of Prüm. This has been one of the main concerns since the early days of Prüm decisions especially for countries with large forensic databases such as the UK (McCartney et al 2011).

Even countries that have fully implemented Prüm have faced difficulties. While volumes of data being exchanged under Prüm have been increasing due to the establishment of new connections among existing members and with the accession of new Member States to the EU, national budgets devoted to international police cooperation have not been increasing. Moreover, while direct access is provided by Prüm to Member States' vehicle data, fingerprint and DNA can only be accessed via follow-up procedures based on a hit notification, requiring further verification and necessitating additional resources, which have not been given adequate attention when considering Prüm expansion (Deloitte 2015).

The EU has tried to address some of the implementation challenges. A Prüm helpdesk was established at Europol in order to support the Member States in relation to the implementation and application of the Prüm Council Decision. However, a low use by the Member States' authorities of the Europol helpdesk has been reported, as well as of the relevant funding instruments, and the targeted support offered initially by the Mobile Competence Team (MCT) (Deloitte 2015). The EU introduced a 'cost-effectiveness principle' and schemes for smaller countries to recover some of their expenditure to join Prüm. Most of the original time limits for implementation have been extended and initiatives to help struggling countries and provide training have been undertaken (Deloitte 2015).

Even though there is funding and support at the EU level, there seems to be a lack of political prioritisation that hinders the implementation of the EU instruments. The current state of affairs reveals varying political commitment across the EU, compatibility issues and a lacking infrastructure for transnational cooperation. There are varying levels of national investment and organisational efficiency which in turn affect the ability to exchange information between jurisdictions and undermine the effectiveness of the entire system (McCartney et al. 2011). It is expected that it may take another several years before Prüm is fully operational, with the implementation likely to be slow and not prioritised by Member States.

Acceptability, legitimacy and accountability concerns

At first sight the above appear to be mainly technical and economic issues however they give rise to questions of acceptability and legitimacy of the Prüm regime (McCartney et al.2011). Prüm obliges all EU member states to establish forensic bio-information databases and to guarantee availability of these databases to other EU States. This is done regardless of national differences in forensic bio-information collection and retention policy. It has been argued that this obligatory exchange which replaces, even in part, any previously voluntary cooperation and exchange of information was made without sufficient consideration and democratic participation from all member states (Bellanova 2008). Critics have argued that the transfer of the Prüm treaty into *the EU acquis* did not fulfil the requirements of democracy and legitimacy (McCartney et al 2011). This is ultimately reflected in the slow implementation and lack of prioritisation in several member states.

Prüm has been described as an example of 'technological development driving policymaking' that does not give sufficient consideration to human rights protection, the democratic process or the trust necessary for the operation of forensic databases and for the cross border exchange of bio- information (McCartney et al 2011). Mutual trust is one of the most important factors in cross-border information exchange. The effective implementation of data exchange provisions has historically faced difficulties generated by a lack of trust between authorities within the same or different member states or the perception that data belong to the authorities that store them (Bellanova 2008). At present, there continue to exist cases of resistance in sharing information between some law enforcement agencies and/or Europol, based on fears of losing control over investigations or even leaks in case information (Deloitte 2015).

Differences in the legal and administrative systems of the Member States and data protection legislation have hindered Prüm implementation and operation the most (Deloitte 2015). While steps toward the necessary technological harmonisation have been taken (Council Resolution 2009/C 296/01; ENFSI 2016) differences in data retention criteria in forensic databases and data protection provisions between the member states challenge standardisation. Human right concerns arise when a state is processing, retaining or sharing personal data which probably should not be on their systems or is not lawfully managed under the EU data protection regime (Soleto-Munoz and Fiodorova 2014). DNA/fingerprint databases in several EU jurisdictions retain the profiles of individuals who are not linked to a crime scene stain or were not formally accused of any criminal offense (Santos et al 2013). At the same time, following the ruling in *S and Marper v United Kingdom* [2008] ECHR 1581, a number of countries (such as the UK, Italy, Poland, Germany), in relation to DNA profiles and fingerprint evidence, are deleting an individual's data if they are found not guilty, charges are dropped or where after an arrest and investigation no further evidence is found.

The practical reality substantiates concerns that 'a virtual EU forensic DNA database constructed with different legislative understandings of proportionality, bodily integrity, right to individual privacy and presumption of innocence, may present an example of increasing

inequalities among EU's "biological citizens"' (Prainsack and Toom 2013). At the same time, the partial implementation of Prüm by some member states contributes to this inequality as the process exposes the citizens of the Member States with larger databases to searches for a variety of offences, including minor ones, far more than those from other countries.

Issues surrounding the retention and exchange of profiles of children and innocent people affect the legitimacy and acceptability of Prüm just as much as the argued lack of accountability and transparent disclosure of its operations (Prainsack and Toom 2013). The Prüm regime is reliant upon both receiving and supplying states checking, and ensuring that the cross border data exchanges comply with their respective national laws. Monitoring Prüm exchanges is left to national data-protection authorities, which can request a log of both automated and non-automated searches and data exchanges. They can then decide upon the lawfulness of the data supply. Indeed, all Member States should be proactive in ensuring that other states cannot and will not abuse data on their citizens (McCartney et al 2011).

Many states have constitutions that protect the right of the citizen not to have data held or exchanged with other authorities unless expressly authorized. While Prüm contains data protection safeguards and measures for individuals to gain information on the data held and how they have been processed; to have personal data corrected if inaccurate and claim damages in the event of any breaches in data protection it is questionable 'whether the individual whose data has been entered onto EU databases or is subject to EU systems of information exchange has in fact any chance of finding out about this, let alone of controlling it' (McCartney et al 2011). It has been questioned whether Prüm provisions 'offer the best guarantees to empower the control of data subjects on their own very sensitive and precious data, especially if data subjects have only an *ex-post* right of information' (Bellanova 2008).

Where personal data move across borders it may put at increased risk the ability of natural persons to exercise their data protection rights against the unlawful use or disclosure of those data. At the same time, national supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers and inconsistent legal regimes (EU Directive 2016/680 rec 75). For these reasons there is a need to promote closer cooperation among national data protection supervisory authorities to facilitate the exchange information with their foreign counterparts and with the Commission in terms of monitoring the consistent application of the safeguards specified in the Prüm decisions and Data Protection Directive 2016.

The implementation and operation of a decentralised network such as Prüm is hard to achieve without some form of centralised decision-making and oversight (Jones 2012). The Prüm regime has been criticised in terms of the lack of oversight of the Prüm process regarding data protection compliance, "proportionality" and lawfulness of data exchanges at a centralised European level (McCartney et al 2011). Prüm has been described as an information exchange mechanism characterised by bureaucracy and complexity which leaves

open the general question of accountability measures and democratic controls (McCartney et al 2011).

Recently there have been developments of EU level initiatives and systems for a more centralised coordination and oversight. The Commission has taken a more proactive role in monitoring the level of Prüm implementation and has shown a commitment to examine whether Member States meet their legal obligations in the area of information systems, whether they make use of existing instruments and if they follow best practices (COM 2016/ 205). In September 2016, the Commission sent letters of formal notice to Croatia, Greece, Ireland, Italy and Portugal for failing to comply with the Prüm Decisions. These are the first infringement procedures initiated for a so-called 'former third pillar instrument' in the field of police cooperation and judicial cooperation in criminal matters (COM 2016/ 670).

In addition the Council has shown a commitment to stimulating the exchange of forensic data via Prüm and improving the quality of forensic data exchanged between all Member States under the Prüm Decisions (Council 10128/16). According to Council's action plan for the creation of a European Forensic Science Area 2016, the Working Party on Information Exchange and Data Protection (DAPIX) is responsible for the EU level oversight of the implementation and operation of Prüm. DAPIX handles the improvement of information exchange between law enforcement authorities of member states and ensures that data exchange is in compliance with current principles and rules on personal data protection. It aims to facilitate the exchange of experience in the implementation and ongoing operation of communication between the systems of member states, in particular mutual assistance in solving the problems that arise not only during implementation, but also in the current work (Council 10128/16). It remains to be seen how these tasks will be carried out and whether the efficiency of the Prüm system, the transparency of the operational procedures and the level of data protection will be improved in the future.

Where next?

The prominence that Prüm Decisions place on cross-border cooperation between Member States in order to combat terrorism and cross-border crime, is one of its most significant contributions. To combat criminal activities EU Member States must cooperate and share information and the Prüm regime is an important step towards the free flowing law enforcement information between EU Member States which offers many benefits to curtail cross-border crime (McCartney 2013). This is achieved and maintained by law enforcement authorities in Member States having access to relevant criminal data through the Prüm databases which requires states cooperating and trusting each other's intelligence, procedures and standards of protection of fundamental rights. In this context Prüm has the potential to enhance trust between Member States and to facilitate growth through cooperation (McCartney et al 2011). Whereas the networks for exchanging DNA profiles and fingerprints hold 'very diverse histories and logics', the Prüm regime has the potential to offer a mechanism for overcoming these differences. Prüm contributes in establishing an EU

'forensic culture' which reorders cooperation in relation to policing cross-border crime (Prainsack and Toom 2013; Wilson 2016). Prüm Decisions provide the grounds for the development (nationally and internationally) of DNA and fingerprint databases, information exchange systems and for a greater European integration among Member States.

Prüm offers a number of benefits that enhance cross border law enforcement cooperation (House of Lords 2015). It simplifies current EU intelligence gathering processes and encourages greater sharing of information as a routine activity which could assist in the early identification of serious offenders and in providing valuable intelligence in relation to counter terrorism investigations. The use of Prüm provides efficiency gains in international searching enabling law enforcement agencies to establish earlier whether an individual is known in another Member State or eliminate a line of enquiry. This leads to early detention and operations to prevent loss of life and/or property. Evidence from countries already operating Prüm shows that it has the potential to identify patterns of crime or criminal associations which are not otherwise apparent (House of Lords 2015). The use of Prüm has the potential to contribute to the resolution of cold cases as the increase in flow of information and data may lead to an increase in hits with unsolved crime data. At the same time, there is currently no other EU mechanism for detecting 'volume crime'. As such Prüm meets a currently suppressed demand. The EU holds several developed DNA/fingerprint databases with the potential to search a dataset in excess of 26 million. Full access to these databases greatly assists the fight against terrorism and organised crime (House of Lords 2015).

Member States seem to recognise the crime solving potential of Prüm as an additional investigative tool for operational police officers (House of Commons 2015). Time and cost effectiveness has been highlighted by a number of Member States, who welcome the need for fewer personnel and resources compared with those required to manage the "classic" DNA and fingerprint exchange mechanism. Furthermore, the verification of hits remains with the requesting Member State and therefore it is more cost and time effective for the requested Member State. However the gap created by lack of implementation by some Member States allows criminals to continue offending across borders without the ability for law enforcement to make use of fast and efficient DNA and fingerprint exchange. When these Member States continue using the "classic" route for fingerprint and DNA exchange - INTERPOL, the Prüm system is jeopardised as it takes additional resources to facilitate both methods of exchange. (Deloitte 2015)

At the same time, heavy reliance on matches for minor crimes or following false or partial hits may divert resources away from preventing crime or conducting thorough investigations (Santos et al 2013). The minimum number of matching loci under the terms of the Prüm system is still six even though it can be calculated and it has been shown in daily practice that six and seven locus matches have a non-negligible chance of being false positive (Home Office 2015). The increasing volume of exchanges of DNA profiles means that the chance of adventitious or false matches may become even more significant (ENSFI 2016). False matches are most likely to occur during the initial 'bulk exchange' of DNA and profiles as this is the stage at which the largest volume will be compared (House of Commons 2015). Any hits need be analysed further by additional DNA-testing before any legal action is

undertaken against a matching person (ENFSI 2016). The lack of a targeted approach (or an approach which is too narrow) would increase the likelihood of individuals with records on DNA and fingerprint databases being suspected after a partial match (Genewatch 2015).

While the problem of false matches is generally acknowledged, the consequences have not always been analysed (McCartney et al 2011). Without a proper consideration, the issue of false hits may become even more significant as the Prüm database becomes larger with the inclusion of new member states and more commonly used. Recent research in France and the Netherlands has found that 26 to 38% of 6 locus hits were true matches, with the result increasing to 82 to 94% of 7 locus hits (Home Office 2015). On the other hand, many Member States' DNA profiles are now stored using the new European Standard Set (ESS) of loci. As a result, with diminishing percentages of profiles with fewer than 10 loci held, the risk of false positives also diminishes (Home Office 2015). It is therefore recommended that Member States could adopt higher standards on DNA loci than the minimum of six stipulated in the Prüm Decisions. Given the convergence towards a higher set of standards across Europe perhaps it is the time for more robust standards and safeguards to be formally incorporated in the Prüm Decisions themselves, ensuring a more uniform application across all EU Member States.

In this context, a useful approach to be taken into account by member states is the one advanced by the UK which officially joined Prüm in May 2016 (Com 2016/809; Council 5650/16). It addresses a number of Prüm concerns discussed above and aims to achieve a safe and fair balance between law enforcement information exchange and human rights protection. According to the UK approach, *only* DNA crime scene profiles with more than *eight loci* will be automatically shared with other Member States on the Prüm exchange so as to ensure that the level of adventitious hits is kept within acceptable and manageable levels. In follow up requests the UK will only share personal data with other Member States relating to a person's profile held in the UK's DNA database *if 10 or more loci are matched* (House of Commons 2015). UK's requirement of 10 loci significantly reduces the likelihood of a false match. This would help to avoid innocent individuals becoming criminal suspects or being dragged into overseas investigations and remove the risk of personal data being unlawfully exchanged between member states. In addition the UK will *only* allow Member States to search the DNA profiles or fingerprints of individuals who have been *convicted* in the UK. In the event of a hit against a person under 18 years old, the UK will only provide personal data if the Member State makes a request for the information using a formal *Letter of Request* via mutual legal assistance channels (House of Commons 2015).

The UK will operate a *proportionality bar* on follow up requests whereby the disclosure of personal data could be denied for not sufficiently serious crimes (House of Commons 2015). This is deemed important in ensuring an adequate balance between law enforcement and individual rights protection and necessary for the management of the volume of exchange. The volume of exchange must be managed carefully, as if the workload increases significantly, and the resources allocated cannot cope with the demand, the system will not work efficiently. Thus it is important that a national search has initially been conducted and

an international element to the crime is considered before a Prüm exchange. In addition, the evidential value of a crime scene profile obtained from a foreign crime scene must be established prior to the release of related demographic data from a matching subject profile held on the domestic database. This should include the 'context' of DNA samples recovered from a crime scene and the type of that sample (House of Commons 2015).

It has been acknowledged by the UK Government that the June 2016 Brexit vote will affect its participation in Prüm and that the UK 'must now reconcile the obligation to implement the Prüm package with the decision to withdraw from the European Union' (House of Commons 2016 a). At the time of writing, the UK Government had decided to implement Prüm as part of the Home Office's planned programme of work in place to deliver biometric services and capabilities (House of Commons 2016 b). It has been suggested that the Government will make some adjustments to its plans to accommodate Prüm, by building additional capability within an existing programme of work. The implementation of Prüm will be undertaken 'as soon as possible', as it has been recognised that the earlier it is implemented the earlier it can be used to prevent and detect crime (House of Commons 2016 b). The House of Commons European Scrutiny Committee has suggested that the UK's future withdrawal from the EU could give rise to the possibility of a bilateral agreement with the EU concerning Prüm being established, similar to those held by the EU with Iceland, Norway, Switzerland and Lichtenstein (House of Commons 2016 (b); House of Lords 2016).

Despite the future of the UK in Prüm and indeed in the EU, the safeguards discussed above address a number of Prüm concerns and as such they could be beneficial for other member states as well. These measures could be given effect at the EU level by imposing additional requirements that go beyond those currently specified in the Prüm Decisions. This could be a useful step in achieving the harmonisation of legal criteria and safeguards between member states. However introducing additional safeguards would require amending the Prüm decisions which arguably may not be practicable at this stage where member states are still to fully implement the Prüm regime. In fact the Commission has declared that it will not consider further developments on the Prüm legal instruments before full implementation by all member states (COM (2012) 732). Yet, adequately addressing Prüm problematic areas remains a priority. DAPIX objectives include an analysis of possibilities to reduce the number of false positive matches with DNA-profiles as well as improving and optimising Prüm follow-up procedures in practice (Council Report 9823/16).

The automated search function of Prüm is a major benefit as it provides immediate feedback on requests. This makes it possible to know where information is available. However, proper follow-up of DNA and fingerprint hits is essential in order to provide information that is actually useful for investigators (Deloitte 2015). There is a heterogeneous picture concerning the tools used to follow up Prüm hits with the majority of member states using Interpol. There are national preferences regarding the channel to use for the follow-up and significantly different approaches seem to exist also *within* the Member States themselves. While numerous stakeholders argue that it is necessary for the continuity of the exchanges that the choice of the follow-up channel be open, it must also be noted that SPOC personnel

currently have to deal with a complex matrix of national preferences for follow-up channels with different Member States. The diversity of follow-up channels can lead to delays in information exchange due to duplication of work or risk of coordination mistakes (Deloitte 2015).

Problems and delays may be significant where Member States' legal and procedural regimes differentiate between information obtained by police and by judicial authorities (Deloitte 2015). Depending on the country, Member States may ask for a given type of information through police co-operation channels if it is considered a police issue in the destination country, while in other countries it may be considered judicial information to be exchanged only through a request for mutual legal assistance. While there has to be increased coherence in the different approaches used for the choice of channel to ensure consistency and speed up the process, binding rules on the choice of channels may not be feasible at this point as a number of pre-conditions must be met, which need to be tackled by several actors. A potential solution could be to promote an existing channel such as Europol's SIENA so that it becomes *de facto* the default channel (Deloitte 2015).

In addition to the above, there are a number of other areas that require further attention if the full potential of Prüm is to be achieved. From a technical perspective, systems currently in use for comparison would benefit from further development. The system used for palm print comparisons for instance, currently does not set out the location within the palm print that a latent palm print has matched, making verification a lengthy process (Home Office 2015). Technical differences hamper interoperability and must be addressed. Functional interoperability can be reached by using agreed definitions of the data exchanged. Technical differences (e.g. formats, messaging standards, message exchange technologies) can hamper interoperability since they impact on reliability, availability and secure transfer that in turn affects the ease with which changes can be implemented (Deloitte 2015).

Due to the lack of using a uniform procedure for the cross-border automated searching and comparison of DNA profiles, methodological irregularities in establishing data exchange statistics arise. Following the requirement of Art.21 of Council Decision 2008/616/JHA to carry out an evaluation of the application of the data exchange pursuant to Chapter 2 of Decision 2008/615/JHA on a regular basis, each Member State compiles statistics on the results of automated data exchange which are annually forwarded to the General Secretariat of the Council to produce an annual summary overview. In 2016 DAPIX identified a number of inconsistencies which call into question the very essence of the statistics that is the comparability, readability as well as reliability of the figures (Council Report 9823/16). The Prüm statistical model should take account of the above differences and all experts at national level need become aware.

Currently there is no formal mechanism to evaluate Member States' implementation of Prüm or its overall impact on the prevention and investigation of crime. The Prüm statistical package does not analyse follow-up work nor is it sufficiently developed to allow conclusions to be drawn on the actual impact of Prüm on investigations (Deloitte 2015). A reason for this is the complexity of Prüm which is not reflected in the data gathering process. The data

currently gathered is on the number of hits and is not comprehensive. Hits need to be verified and those which are successfully verified are only an unknown subset of the overall hit count. Moreover, once the exchange is completed, it would be very beneficial to look at the number of cases in which information obtained following a hit was actually used in criminal proceedings. Such data could be used to assess the effectiveness of the Prüm system and its impact in the fight against cross border crime. Currently there is no method, other than individual analysis of each case, to discover whether a hit was evidential or provided a useful investigatory lead or not (Home Office 2015).

While monitoring the actual outcome of Prüm exchanges in judiciary proceedings is challenging, statistics on the actual number of hits that were followed up at all in investigations (irrespective of the specific impact on judiciary proceedings) seem in principle to be easier to produce. However, as there is no designated channel for Prüm follow-up and the choice of channel varies sometimes even within the same Member State, challenges exist in producing accurate and useful statistics (Deloitte 2015). These issues need be addressed so as to enhance the transparency and accountability of Prüm which will ultimately be reflected in the trust necessary for the operation of cross border exchange systems.

Last but not least, there is need for training and education of all actors involved in the Prüm process. Prüm relies on Member States sending fingerprints/DNA/VRD for searching against other Member States databases, which will only work effectively if those working in law enforcement are aware of this capability (Home Office 2015). There is need to raise the awareness of Member States' national laws that impacts on the Prüm process as well as to share best practice so that non-operational Member States can benefit from the experience of others (Deloitte 2015). Currently there are gaps in the overall training offered and the quality of delivered training is not always sufficient. It has been reported that the awareness of field officers of the possibilities for exchanging information is too low because the topic is not sufficiently covered at the police academy or covered too theoretically (Deloitte 2015).

While a variety of different actors are involved in providing training there is currently no overarching training strategy at the EU level. Many Member States do not have a training strategy identifying needs and rather offer training on an ad hoc basis (Deloitte 2015). Strategies need be developed at the EU and national level that define knowledge needs and training gaps as well as set out concrete plans on how to cater for these needs. Consideration should be given to developing specific training packages that cover all channels and instruments that are relevant for information exchange. There is a need to make full use of the existing training offers and for the offers to be enhanced where necessary. To achieve this, the Member States, the Commission, DAPIX, and Europol need to contribute and work together.

Conclusion

During the past decades, the EU member states as well as other countries in the world have increased their efforts to achieve a closer cooperation in combating terrorism, organised

crime and illegal immigration. The Prüm network was established to provide mechanisms and the infrastructure to achieve these goals through the cross border exchange of DNA profiles, fingerprints and vehicle registration data. Prüm network simplifies intelligence gathering and increases criminal detections - particularly regarding organised crime and terrorism. It provides for efficiency gains in international searching and a more efficient response by law enforcement agencies. It increases the resolution of cold cases and provides the only cross border mechanism in the EU for detecting volume crime. However Prüm continues to present challenges of a technical and scientific nature as well as legal, ethical and socioeconomic concerns.

In order to maximise its potential, it is important to enhance the necessary dialogue and cooperation between member states so as to address challenges posed by Prüm through balanced measures. Such measures could include additional safeguards as to the type of data exchanged and data protection, further technological improvements as well as an increased awareness of Prüm capabilities and of national legislation that impacts on the Prüm process through training and education. The gap created by the lack of implementation by some Member States need be addressed as the duality of data exchange methods jeopardises the Prüm system by draining resources. An EU level oversight of Prüm, greater transparency and accountability, alongside the harmonisation of national legislations on DNA retention and of safeguards on fundamental rights protection, would enhance the trust and dialogue necessary for transnational cooperation.

References

Bellanova, R. (2008) 'The "Prüm Process:" The Way Forward?' in *Security vs Justice? Police and Judicial cooperation in the EU eds* E.Guild and F.Geyer, 203-221, Aldershot: Ashgate

Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime

Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation particularly in combating terrorism and cross-border crime

Council Decision 2007/533/JHA on the establishment, operation and use of the second generation Schengen Information System (SIS II)

Council Decision 2009/371/JHA establishing the European Police Office (Europol) available at https://www.europol.europa.eu/sites/default/files/council_decision.pdf accessed 09.02.2017

Council Framework Decision 2006/960 JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union

Council Framework Decision 2009/905/JHA on accreditation of forensic service providers carrying out laboratory activities

Council of the European Union (2009) Resolution 2009/C 296/01 on the exchange of DNA analysis results

Council of the European Union (2009) 'Draft Council Conclusions on an Information Management Strategy for EU internal security' (Council 16637/09) available at http://register.consilium.europa.eu/pdf/en/09/st16/st16637.en09.pdf accessed 28.01.2017

Council of the European Union (2016) '"Prüm Decisions" - Presidency progress report' (Council 9823/16) available at http://data.consilium.europa.eu/doc/document/ST-9823-2016-INIT/en/pdf accessed 28.01.2017

Council of the European Union (2016) 'Council Conclusions and Action Plan on the way forward in view of the creation of an European Forensic Science Area' (Council 10128/16) available at http://data.consilium.europa.eu/doc/document/ST-10128-2016-INIT/en/pdf accessed 09.02.2017

Council of the European Union (2016) Renewed European Union Internal Security Strategy and Counter Terrorism Implementation Paper: second half of 2016 (Council 11001/16) available at http://www.statewatch.org/news/2016/sep/eu-council-intermal-security-11001-16.pdf accessed 09.02.2017

Council of the European Union (2016) Notification of The UK participation in Council Decisions 2008/615/JHA and 2008/616/JHA ("Prüm Decisions"), and Council Framework Decision 2009/906/JHA (Council 5650/16) available at http://data.consilium.europa.eu/doc/document/ST-5650-2016-INIT/en/pdf accessed 20.04.2017

Deloitte: European Commission Directorate-General Migration and Home Affairs (2015) 'Study on the implementation of the European Information Exchange Model (EIXM) for strengthening law enforcement cooperation' (26 January 2015) available at http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/police-cooperation/general/docs/eixm_study_-_final_report_en.pdf accessed 09.02.2017

ENFSI (2016) DNA-Database Management Review and Recommendations, ENFSI DNA Working Group available at http://enfsi.eu/wp-content/uploads/2016/09/final_version_enfsi_2016_document_on_dna-database_management_0.pdf accessed 09.02.2017

European Commission (2010) 'Overview of information management in the area of freedom, security and justice' COM (2010)385 available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0385:FIN:EN:PDF accessed 09.02.2017

European Commission (2012) Report from the Commission to the European parliament and the Council on the implementation of Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (the 'Prüm Decision') COM (2012) 732 available at http://ec.europa.eu/transparency/regdoc/rep/1/2012/EN/1-2012-732-EN-F1-1.Pdf accessed 09.02.2017

European Commission (2015) Fact Sheet 'European Agenda on Security - State of Play' Brussels, 17 November 2015 available at http://europa.eu/rapid/press-release_MEMO-15-6115_en.htm accessed 09.02.2017

European Commission (2016) 'Stronger and Smarter Information Systems for Borders and Security' COM(2016) 205 available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2016%3A205%3AFIN accessed 09.02.2017

European Commission (2016) 'First progress report towards an effective and genuine Security Union' COM (2016) 670 available at https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/legislative-documents/docs/20161012/first_progress_report_towards_an_effective_and_genuine_security_union_en.pdf accessed 09.02.2017

European Commission Decision (EU) 2016/809 of 20 May 2016 on the notification by the United Kingdom of Great Britain and Northern Ireland of its wish to participate in certain acts of the Union in the field of police cooperation adopted before the entry into force of the Treaty of Lisbon and which are not part of the Schengen acquis

EU Directive 2016/680 on the protection of natural persons with regard to processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and on the free movement of such data repealing Council Framework Decision 2008/977/JHA

GeneWatch UK (2015) 'Sharing DNA profiles and fingerprints across the EU requires further safeguards' Genewatch UK Briefing (December 2015) http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/Pruembrief_Nov15_fin.pdf accessed 09.02.2017

Home Office (2015) 'Prüm Business and Implementation Case' (November 2015) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/480129/prum_business_and_implementation_case.pdf> accessed 09.02.2017

House of Commons European Scrutiny Committee (2015) 'Cross-border law enforcement cooperation - UK participation in Prüm' available at <http://www.publications.parliament.uk/pa/cm201516/cmselect/cmeuleg/342-xii/342xii.pdf> accessed 09.02.2017

House of Commons 2016 (a) 'Parliamentary Committee on the UK's participation in Prüm following Brexit' available at

http://www.publications.parliament.uk/pa/cm201617/cmselect/cmeuleg/71-vi/7103.htm accessed 05.05.2017

House of Commons 2016 (b) 'Cross-border law enforcement cooperation—UK participation in Prüm' available at http://www.publications.parliament.uk/pa/cm201617/cmselect/cmeuleg/71-vi/7122.htm accessed 05.05.2017

House of Lords European Union Committee (2015) 'The United Kingdom's participation in Prüm' available at http://www.publications.parliament.uk/pa/ld201516/ldselect/ldeucom/66/66.pdf accessed 09.02.2017

House of Lords European Union Committee (2016) 'Brexit: future UK-EU security and police cooperation' available at http://www.parliament.uk/brexit-security-police-cooperation accessed 05.05.2017

INTERPOL Databases https://www.interpol.int/INTERPOL-expertise/Databases accessed 08.05.2017

Jones, C. (2012) '"Complex, technologically fraught and expensive" - the problematic implementation of the Prüm Decision' Statewatch analysis available at http://www.statewatch.org/analyses/no-197-prum-implementation.pdf accessed 09.02.2017

McCartney C., Wilson T., Williams R. (2011) 'Transnational exchange of forensic DNA: viability, legitimacy, and acceptability' European Journal on Criminal Policy and Research 2011, 17: 305–322. doi:10.1007/s10610–011–9154-y

McCartney, C. (2013) 'Opting in and opting out: doing the hokey cokey with EU policing and judicial cooperation' Journal of Criminal Law 77(6), 543-561

Prainsack, B. and Toom, V. (2013) 'Performing the Union: the Prüm Decision and the European dream' *Studies in the History and Philosophy of Science*, 44 (1), 71-79

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA

Santos, F., Machado, H. and Silva, s. (2013) 'Forensic DNA databases in European countries: is size linked to performance?' Life Sciences, Society and Policy Journal 9: 12 doi:10.1186/2195-7819-9-12

Soleto Muñoz, H. & Fiodorova, A., (2014). DNA and Law Enforcement in the European Union: Tools and Human Rights Protection. Utrecht Law Review. 10(1), 149–162 DOI: http://doi.org/10.18352/ulr.262

The Hague Programme: Strengthening Freedom, Security and Justice in the EU (2005/C 53/01) available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2005:053:0001:0014:EN:PDF accessed 09.02.2017

The Stockholm Programme – An Open and Secure Europe Serving and Protecting Citizens (2010/C 115/01) available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:EN:PDF accessed 09.02.2017

Topfer, E. (2011) '"Network with errors": Europe's emerging web of DNA databases' Statewatch Journal Vol.21(1) available at http://www.statewatch.org/analyses/no-134-dna-databases.pdf accessed 09.02.2017

Wilson, T. (2016) 'Criminal Justice and Global Public Goods: The Prüm Forensic Biometric Cooperation Model' The Journal of Criminal Law 2016, Vol. 80(5) 303–326