The Road from *S. and Marper* to the Prüm Treaty and the Implications on Human Rights
Katina Michael

**Introduction**
This chapter investigates the implications of the *S. and Marper v United Kingdom* ruling by the European Court of Human Rights (ECtHR), which found that the UK Government’s current deoxyribonucleic acid (DNA) retention policy breached Article 8 of the *European Convention on Human Rights* (ECHR) (Council of Europe 2008). The aim of this chapter is to look beyond the changes that have been instigated in Britain, since the landmark decision by the ECtHR was made, and toward the legal and human rights implications of the sharing of DNA data across the borders of European Union member states. Of significance here are the outcomes of the Prüm Treaty of 2005, which initially saw seven countries, not including the UK, agree to share DNA data, fingerprint and vehicle registration data for the purpose of countering acts of terror and bringing criminals to prosecution. By June 2007, the provisions of Prüm had found their way into the legislative framework of the European Union at large. This setting is contrasted against a backdrop of an increasing number of organisations at the supranational level that have been tasked with overseeing the fundamental protection of human rights, especially in the case of minors, paying attention especially to an individual’s right to privacy and personal data protection. The book chapter is divided into four parts: an overview of the Prüm Treaty, a discussion on the retention of DNA and fingerprint samples in EU member states, the implications of the *S. and Marper* case ECtHR ruling in Britain and the wider EU, and the protection of the human rights of EU citizens.

**The Prüm Treaty**
The Prüm Treaty of 2005 was a German-led initiative to increase cross-border cooperation for the combating of terrorism, crime and illegal immigration. It is sometimes referred to as Schengen III, for the particular reason that the same five parties (Belgium, Germany, Spain, France, Luxembourg, the Netherlands and Austria) collaborated in 1985 on the Schengen Agreement and, later in 1990, on the Schengen Convention (House of Lord 2007). The Agreement was hastily signed, raising fundamental questions concerning the main provisions of the Treaty (Boehm 2009, Donnelly 2007), which focused on reciprocal access of Member States to national databases containing biometric data (such as DNA profiles and fingerprints), as well as vehicle registration data (European Parliament 2007). Although little time was allocated to debating the contents of the Agreement, by June 2007 the provisions had found their way into the legislative framework of the European Union (EUROPA 2007). Even the United Kingdom reluctantly signed the Convention, although it has only partially agreed to the contents (European Digital Rights 2007).

*The Prüm Treaty Biometric Provisions versus Schengen Information System II*
Chapter 2 of the Prüm Treaty contains provisions that stipulate contracting parties must ensure both availability and access to data such as DNA identifiers through automated online searches. Article 2(1) states that: ‘Contracting Parties shall ensure the availability of reference data from their national DNA analysis files’ and that ‘[r]efERENCE DA
only include DNA profiles established from the non-coding part of DNA and a reference.’ It is clear that the reference data must not contain any information that can identify the subject. To understand the legal implications of this provision one must reflect on the Schengen Agreement, especially Title IV.

In Articles 94-100, the implementation of the Schengen Information System (SIS) is described in detail. While the SIS was created as a compensatory measure to allow for the free movement of persons, it increasingly became used as a tool for police cooperation between Member States in the EU, whose data could be used for purposes other than those initially envisaged (European Parliament 2003). The idea behind the second phase of the SIS was to introduce a more powerful system that could enhance police cooperation across borders. However, the problem with the SIS II implementation and the SIRENE (Supplementary Information Request at the National Entry) network was that no clear legal framework on police cooperation across borders had been laid out in Article 30 of the Treaty on the European Union. Some observers believe that the Prüm Treaty was a way to overcome these issues to enter more rapidly into an environment of sharing data across borders, beyond the technical capabilities of SIS II. However, there seems to have been a deliberate exclusion of other types of data from the Treaty, including ballistics, communications data and identification data in civil registers (House of Lords 2007).

The provisions for data storage in the original Schengen Information System included two types of data - subject specific (for example, person-related data) and object specific (for example, vehicle data). Examples of person-specific data include: surnames, aliases, physical characteristics not subject to change, date and place of birth, sex, nationality, whether persons concerned are armed or violent, reason for alert and the action to be taken. Examples of object/vehicle-specific data include: stolen motor vehicles, firearms which have been misappropriated, blank official documents which have been stolen, issued identity papers which have been stolen and suspect banknotes. In addition to the SIS base data, the Prüm Treaty stipulates additional person-specific data, such as biometric data. DNA and fingerprint (dactyloscopic) data identification patterns are two types of physiological biometrics (Koblinsky et al. 2005). The Treaty also grants EU states cross-border access to data, subject to the principle of availability. In urgent situations, officers from one Contracting Party may, without another Contracting Party's prior consent, cross the border so that they can take provisional measures necessary to avert imminent danger to the physical integrity of people. This type of measure is known as hot pursuit.

Cross-border Personal Data Matching Capabilities in the EU after the Prüm Treaty
The main objective of the SIS was to exchange data on certain categories of people and lost or stolen goods. According to Articles 95-100 of the Schengen Agreement, the reasons for triggering an alert included, but were not limited to: arrest for the purposes of extradition, to find a missing person whose detention has been ordered, arrest for the purpose of appearing in court, discrete surveillance and specific checks (Article 99) and in the case of aliens, who in most cases have not complied with provisions governing

> Every national alert that is “Schengen relevant” should in principle be introduced in the SIS. However, in order to be able to execute the alert, it is necessary that the alert is correct, as complete as possible and traceable. Finally, it should be borne in mind that when a Schengen State executes an alert, it has the right to expect that the issuing Schengen State will follow up the hit. Not doing so without a valid (legal) reason will negatively impact on the willingness of (local) authorities to use the SIS and maximize its potential.

Similarly, along the lines of the SIS II and SIRENE networks, the Prüm Treaty maintains that the first contact between States is on a “hit/no hit” basis (Figure 1.1). Article 3(2) states that:

> Should an automated search show that a DNA profile supplied matches a DNA profile entered in the Contracting Party's file searched, the searching contact point shall receive automated notification of the hit and the reference. If no match can be found, automated notification of this shall be given.

If no DNA sample is available of a given person during ongoing investigations or criminal proceedings, then as stipulated in Article 7 ‘the requested Contracting Party shall provide legal assistance by collecting and examining cellular material from that individual and by supplying the DNA profile obtained.’ Article 3 is clear that ‘search powers may be exercised only in individual cases and in compliance with the searching Contracting Party's national law.’

However, there are complications in practice to the process of providing DNA data first as information and then as evidence (Pereira 2008). Some of these issues were discussed in depth at the European Conference on International DNA Data Exchange in Criminal Justice in June 2008 held in Maastricht/Heerlen, The Netherlands. The crux of the matter is that a ‘hit’ on DNA data will almost always end up being used as exclusive evidence in a court of law, but in the Prüm mechanism there are additional procedural steps that are required, as a DNA match is merely considered ‘information’ (Open University 2008). Some of the key questions that the Conference sought to address included:

1) What would be a proper implementation of the Prüm mechanism?
2) Would Prüm act to combat acts of terror, or would it ultimately be used to investigate and prosecute lower level crimes across borders?
3) Is the data protection sufficiently safeguarded under the new instrument?
4) Are we moving into the direction of one European database for DNA data?

**The S. and Marper v United Kingdom Ruling**

The *S. and Marper v United Kingdom* landmark case, when analysed within the context of a supranational Europe provides some interesting material, particularly when
superimposed against the proceedings of the Prüm Treaty. Figure 1.2 contains a timeline showing decisions by various courts in the S. and Marper case, as well as key stages in the Prüm Treaty’s enactment and implementation. On the 04 December 2008, the judgment of S. and Marper v United Kingdom was delivered by the European Court of Human Rights, which found that the UK Government’s current DNA retention policy breached Article 8 of the European Convention on Human Rights relating to privacy (Liberty 2009, Sankey 2009, McCartney 2010, Michael 2010). Article 8(1) of ECHR states: ‘[e]veryone has the right to respect for his private and family life, his home and his correspondence’. Since the decision by the ECtHR, there has been some confusion over the ruling’s impact on the practices, policies and laws of the United Kingdom, especially with respect to the indefinite retention of a suspect’s personal data, and more widely within the context of the European Union at large (Raif-Meyer et al. 2008). The Court has the power to award damages to the claimants but the ruling is not automatically binding on the United Kingdom or other members.

In fact, Lord West of Spithead reported in the UK Parliament on 18 May 2009 that ‘[o]ther than the relevant fingerprints and DNA samples belonging to S and Marper, no fingerprints or DNA samples ha[d] been destroyed as a result of the judgment of the European Court of Human Rights’ (Hansard 2009). Lord West of Spithead went on to state that :

> Article 41 of the Convention for the Protection of Human Rights and Fundamental Freedoms provides that if the court finds that a violation has occurred, just satisfaction must be made to the injured party. The application of the judgment to others in similar situations must be considered in the light of the full content of the judgment. The judgment does provide for the member state to consider the scope for achieving a proper balance with the competing interests of tackling crime and preserving respect for private life. (Ibid)

**The United Kingdom’s Response to the S. and Marper Judgment**

The United Kingdom’s response to S. and Marper, to change sections of the Police and Criminal Evidence Act 1984 (the PACE) in order to keep pace with the decision, have been slow. For now, PACE remains in force and unchanged (Mery 2009). On 07 May 2009, the Home Secretary launched the public consultation Keeping the Right People on the DNA Database. The consultation paper sets out how the Government hopes to implement the S. and Marper judgment and the proposed framework to ensure the safeguarding of the rights of UK citizens (Home Office 2009). The question now is what happens to those samples collected prior to the ECtHR ruling or during the consultation process (Almandras 2009). For example, in the future, what will be the process for determining which samples to destroy and which to retain (Whitehead 2009)?

In 2001, Section 64(1A) of PACE was substituted with Section 82 of the Criminal Justice and Police Act. The change to legislation meant that a suspect of a crime would have his fingerprints and samples permanently stored on the police national computer (PNC), even after having been acquitted or never charged of any crime (Beattie 2009, Simon 2003).
As of December 2008, 5.3 million DNA profiles were retained in England and Wales (Anonymous 2008). A further 857,000 fingerprint and DNA samples of innocent citizens were also stored (Travis 2008). This is a grossly disproportionate number of profiles and samples when one considers that most other nations do not collect profiles of more than 2% of their citizens. Recordable offenses for which a DNA can be obtained under the 2008 UK laws included crimes which carry a custodial sentence not excluding petty misdeeds such as begging, being under the influence of alcohol, or acting in a disorderly fashion (Camp and Dierickx 2007).

Perhaps the greatest injustice of the U.K. legislation to surface from the S. and Marper case related to the collection and storage of DNA samples and profiles of persons who had not - and may never be - convicted of a crime (Lynch et al. 2008). For some, especially those wrongly apprehended, having their DNA permanently stored on the National DNA Database (NDNA) would almost certainly lead to a feeling of bitterness or dislike or hatred for the State and especially the U.K. Police. Among the one million innocent people whose DNA sample has been taken are an estimated 100,000 innocent children (Action on Rights for Children 2007). What are these persons to think and feel as they advance in age? What does it mean about their future, or employment opportunities requiring security checks? And how might their experience with Police impact them later in life? Psychologists have pointed out that someone treated like a criminal may retaliate as if they were one: ‘[b]ecause it feels like someone is punishing [them] by making [them] feel guilty, [they] often have an urge to retaliate against those who do’ (Stosny 2008).

But beyond the psychological repercussions on the individual stemming from what some refer to as “emotional pollution” is the effort that a person must go through to get their details removed from the NDNAD, a process that was almost impossible until the S. and Marper judgment (Geoghegan 2009). Since 2004, in England, Wales and Northern Ireland records are removed and DNA destroyed only under ‘exceptional circumstances’ (Genewatch UK 2009). And given the profiles on the NDNAD belong to individual police forces, innocent persons whose profiles remain on the NDNAD and who wish to have them removed need to appeal to their Constabulary directly. This is despite that in the beginning of 2009 the Association of Chief Police Officers of England Wales and Northern Ireland (ACPO) asked officers to ignore the ECtHR ruling (Travis 2009).

At the end of March 2009, Lord West of Spithead noted that the NDNAD contained DNA profiles and linked DNA samples from 4.9 million individuals, of which an estimated 4.6 million were from English and Welsh forces (more than 7 per cent of the U.K. population) (Hansard 2009). However, this figure should be compared with those cited on 27 October 2009 in Parliament, which indicated that at the end of March 2008, there were a total of approximately 5 million profiles on the NDNAD and by March 2009 approximately 5.6 million. According to population statistics from August 2009, obtained from the Office for National Statistics, there are about 61.4 million people residing in the U.K., which means that the NDNAD contains profiles of more than 8.36 per cent of the total population in the United Kingdom (Office for National Statistics 2009).
This figure is, however, is a rather conservative estimate, when one considers that Scotland has a different legislative requirement regarding the retention of DNA profiles.

Such figures indicate a number of points: First, the size of the UK databank is growing at over 560,000 profiles per annum, which is at keeping with the rate of 40,000 to 50,000 samples per month. Secondly, one in nine persons in England, Wales and Northern Ireland is registered on the databank. Thirdly, and more to the point, there are 507,636 DNA profiles which are of unknown persons. This either means that these samples have been collected at crime scenes and have not been individually identified alongside ‘known’ persons, or that potential errors exist in the NDNAD itself.

**DNA Data Retention and Standards Across EU Member States**

In some EU member states like Portugal there are no specific laws governing the retention of DNA, even in such cases as pedophilia (Kierkegaard 2009). In fact, when one compares the laws between countries, we find a major problem in how the Prüm Treaty will take effect in practice. Table 1.1 presents a fresh analysis of how DNA retention and destruction differ between EU member states, categorized by four levels of retention. Herein lies a fundamental flaw of the Prüm mechanism: how can one Contracting Party provide access to another Contracting Party for DNA sample data-matching, when that Party does not retain DNA samples of criminals in a database nor has a law that even governs this process? While it should be noted, for example, that the majority of the Council of Europe Member States allow for the compulsory taking of fingerprints and DNA samples in the context of criminal proceedings, not all of them do. Among the EU countries that do have provisions are: Austria, Belgium, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Luxembourg, the Netherlands, Poland, Spain and Sweden. For well-known international lawyer Professor Sylvia Mercado Kierkegaard, the laws and shortcomings of the Prüm Convention surround the fact that there are no EU policy standards for the collection and retention of genetic databases (Kierkegaard 2008).

Table 1.1 NEAR HERE

**Who has Full Access to DNA Databanks?**

What is interesting to note is that a number of European Union states do not only collect DNA profile data but also retain the DNA celluloid sample gathered. This is in contrast to United States databases that for the greater part contain profile data alone. Another problem with the lack of standardization pertains to the authority granted to police to gather DNA data at a crime scene (Camp and Dierickx 2007). In some countries, including Lithuania, Sweden, and Slovakia, DNA samples cannot be gathered from minors or persons who are mentally ill, even if they are suspected of a serious crime. When we compare also who has full authority to access DNA databases in different EU states, we find in some countries that forensic divisions are given complete access rights and in other countries law enforcement officers or judicial officials are entrusted with this power. Only in Germany and Denmark are both forensic divisions and law enforcement given full access to the databases. This provides an additional complication for
Contracting Parties exchanging details of DNA matches under the Prüm mechanism, as contact must be made with the right authoritative power for a given national jurisdiction.

**Cases Related to DNA Data Pertaining to Article 8 ECHR**
The *S. and Marper* case, while now well-known for the decision made by the Strasbourg court, is not the first case to highlight issues to do with personal data, usage, data protection and rights to privacy under the European Convention on Human Rights. A number of other cases have highlighted the problems associated with the collection of DNA data, collection and retention (especially after acquittals or discontinuance of a case) with respect largely to Articles 8 and 14 of the ECHR. In 1983, three cases, *McVeigh v United Kingdom, O'Neill v United Kingdom, Evans v United Kingdom*, were heard by the ECtHR with respect to actions required in investigating terrorism and detaining persons, including the acts of questioning, searching, photographing and fingerprinting persons detained to prevent a serious crime. While the cases did not refer directly to DNA evidence, they did discuss another form of biometric - fingerprinting. Two more relevant cases include *Amann v Switzerland* [1998] and *Rotaru v Romania* [2001]. Nick Taylor writes about these cases within the context of exploring policing, privacy rights and frameworks within which the police should operate in order to respect the right to private life (Taylor 2003).

The case which can be considered a precursor to *S. and Marper v United Kingdom* is a 2001 case known as *R. v B.*, which was ultimately heard in the House of Lords. In this case, the interpretation of the PACE Act 1984 (s. 64(3B)(b)) was under scrutiny. In short, a DNA sample that should have been destroyed following an acquittal of B on a charge of rape was used to connect B to an unrelated burglary.

Subsequently, the DNA evidence was found inadmissible because samples had been retained unlawfully (2001). In the case notes of *R. v Weir* [2000] it is stated:

> W was arrested in June 1998 on the basis of the DNA match which linked him to the attack. He provided two samples of blood which confirmed the match and was consequently convicted of murder, burglary and assault and sentenced to life imprisonment. W appealed against his conviction and contended that not only had he been entitled to the destruction of his first sample under s. 64(1) but that s. 64(3B)(b), as inserted by the Criminal Justice and Public Order Act 1994, excluded the admission of any evidence which had resulted from a link between the first sample, which should have been destroyed, and the second sample and any information derived therefrom.'

**Protecting the Individual’s Right to Privacy in the EU**
Privacy can be defined as the interest that individuals have in sustaining a personal space, free from interference by other people and organizations (Markesinis 1999). The importance of privacy today is reflected in that it is fundamentally embedded in all human rights-related documents and treaties applicable to Europe, such as the *Universal Declaration of Human Rights* (1948), the *European Convention on Human Rights* (1950), and the *Charter of Fundamental Rights* (2000) (Bygrave 1998). With the application of modern computing technologies in the law enforcement field post-1990s, the ability to
collect, process, and store large numbers of fingerprint minutiae, cellular samples and DNA in data warehouses (Bieber 2006) has been significantly progressed (Neil 1999). Today, there is the ability to not only conduct individual profiling (Glod 2004) but also social sorting (Lyon 2002) and familial searching (Lazer 2004). The ability to cross-match and data mine personal information that is stored for purposes other than what it was intended for is known as ‘function creep’ (Chandra and Calderon 2005) and this remains one of the greatest risks, alongside identification theft (Skene 2005), associated with amassing public databases and registers (Meek 2002). The law is supposed to protect the rights and freedoms of individuals but on occasion it has been found to be in breach of fundamental human rights (Gunning and Holm 2005). At least there needs to be some balance struck between principles of proportionality, subsidiarity, accountability, finality, availability and accessibility (Farrar 2001).

The findings of the inquiry indicate that there is a mismatch, especially in the number of years that personal DNA data is retained between member states in the EU and how that data is used. To allow DNA data sharing across borders, when definitions over what constitutes the right to retain a DNA sample differ so widely, as well as the length of retention, would be creating a situation destined for disaster. All this in light of the problems associated with DNA evidence to begin with, the potential for errors in sampling, the risks inherent in data losses and the potential unanticipated future uses without the commensurate safeguards in place, are catapulting the EU into a surveillance society.

**Towards the Harmonisation of State DNA-related Laws for Criminal Proceedings**

The complexity of having laws at both the national and supranational level is evident from the legislation and cases that have been reviewed in this chapter with respect to DNA information/evidence (Roberts and Taylor 2005). Exacerbating this issue is the problem with the powers of different European-centric courts - the ECtHR, which is binding on the Council of Europe’s 47 Member States on the one hand, and the European Court of Justice (ECJ), entwined in the Third Pillar (Hatzopoulos 2008), and relevant to 27 Member States of the European Union. Consider, for example, the role of the Commissioner for Human Rights versus the roles of National and European Data Protection Supervisors linked to Justice and Home Affairs (Hammarberg 2008, EUROPA, EUROPA 2009). Increasingly, to borrow from the words of Sir Brian Neil (1999: 28), national judges are being referred to decisions reached in other EU member state jurisdictions and invited to consider different systems of law, suggesting ‘a need to try over a period of time to harmonise the laws of different states in such areas of the law as freedom of speech and freedom for an individual’s private life and affairs.’

**Conclusion**

There is, to some extent, some jostling occurring between national laws and European Union wide laws; indeed, while it is national governments who make decisions to give powers to European bodies (Richardson 2006), once ratified, European treaties and associated legal texts ‘take on a life of their own.’ Alter (2001: 203) writes:

> [n]ational governments decide when to give new powers to European bodies, thus where to expand the reach of European law over national policy. Their legislative
powers in the Council, and their treaty-making powers in intergovernmental conferences, ensure that member states in some respects stay in charge of the overall process of legal integration. But once written, European legal texts take on a life of their own. In theory, member states always have the option of revising texts should they be unhappy with the outcome. But in practice, changing existent legislation is difficult to do and often politically unfeasible.

How participatory of EU Member States the Prüm Treaty actually was is debatable, given it was initially signed by only a quarter of the members in 2005. But all this is now of little significance, as all EU members are well ‘on-board’ and the Prüm mechanism has taken on a life of its own (Slaughter and Mattli 2006). No longer are we so preoccupied with Prüm but the way in which Prüm and other decisions like *S. and Marper v United Kingdom* will impact national laws towards standards and harmonisation in DNA profile and sample collection, retention and destruction (Lawson 2005). This raises questions requiring socio-ethical evaluations which have been completely ignored from the outset (Camp and Dierickx 2007). For now, we might only ponder on the dawn of a fully-fledged surveillance society (Lyon 2001) and the repercussions of the Prüm provisions (Pereira 2008).

**Notes**

1 Prüm Convention Between 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 on the Stepping up of Cross-border Cooperation, Particularly in Combating Terrorism, Cross-border Crime and Illegal Migration.

**Bibliography**

**Secondary Sources**


presentation at the IEEE Symposium on Technology and Society, University of Wollongong, Wollongong, 7-9 June: 48-60.


Primary Sources

Action on Rights for Children (2007) ‘How Many Innocent Children are Being Added to the National DNA Database?’.  


R. v Weir (Michael Clive) (CA (Crim Div)), Court of Appeal (Criminal Division), 26 May 2000.


