in:ex

Converging and conflicting ethical values in the internal/external security continuum in Europe

European Commission, 7th Framework Programme

CENTRE FOR EUROPEAN POLICY STUDIES

Thinking ahead for Europe

INEX Policy Brief

# Global Data Transfers:
## The Human Rights Implications

**Elspeth Guild**

**No. 9 / May 2010**

SEVENTH FRAMEWORK PROGRAMME

Research for this Policy Brief was conducted in the context of Work Package 9 of INEX, a three-year project on converging and conflicting ethical values in the internal/external security continuum in Europe, funded by the Security Programme of DG Enterprise of the European Commission's Seventh Framework Research Programme. The project is coordinated by PRIO, International Peace Research Institute in Oslo. For more information about the project, please visit: www.inexproject.eu

PRIO

International Peace Research Institute, Oslo

# GLOBAL DATA TRANSFERS:
# THE HUMAN RIGHTS IMPLICATIONS

*INEX POLICY BRIEF NO. 9 / MAY 2009*

**ELSPETH GUILD***

## Introduction

We live in a world where global data transfers are presented as a norm; just part of life. Occasionally, some surprise is expressed at reactions to data transfer across countries, for instance when the European Parliament rejected the SWIFT Agreement[1] in February 2010, thus bringing to a halt the transfer of data on EU nationals' banking transactions to the US authorities. Some commentators have expressed dismay at this 'unnecessary' move, which impedes the fight against financing terrorism. Others point to the problems that have arisen as a result of a too easy transfer of personal data across borders.

It is important to bear in mind what is at stake in this discussion. As an illustration, Maher Arar, a Canadian citizen, was stopped on his return to Canada via the USA in 2002, detained, questioned and then sent to Syria, where he was subjected to torture for one year before the Canadian authorities sought his return to Canada, which was granted. According to the Canadian Royal Commission which examined the facts of the case, the reason Mr Arar was detained by the US authorities was a result of information the Canadian intelligence services had provided to their US counterparts, but which was unreliable. The Canadian authorities acknowledged their part in Mr Arar's suffering and awarded him CAN$11 million (including legal fees). Subsequent investigations into other Canadians who suffered similarly as a result of lax rules on data sharing across borders have resulted in very substantial damages settlements as well.[2] The Swedish authorities permitted US and Egyptian authorities to bring a plane to Swedish territory and arrested and handed over to the foreign authorities two Egyptian nationals Amandine Scherrer, Mr Agiza and Mr Azery, both of whom had sought refugee status in Sweden. The authorities allowed the men to be subject to inhuman and degrading treatment, if not torture, on Swedish soil before being taken to Egypt. Following adverse findings by both the UN Human Rights Committee and the UN Committee against Torture, the Swedish authorities settled damages claims in respect of both men last summer.[3]

In the UK the case of Binyamin Mohammed is still outstanding in the courts. He was arrested by militia in Pakistan in April 2002, sold to the US forces and then tortured both in Afghanistan and elsewhere before ending up in the US base in Guantanamo Bay. The question for the UK courts is the degree of knowledge, or as some might suggest complicity, that there may have

* Elspeth Guild is Senior Research Fellow at CEPS.

[1] This enabled agencies in the EU to provide information to their US counterparts on all electronic bank transfers in Europe, processed by the Belgium-based company, SWIFT.

[2] Audrey Macklin, *Transjudicial Conversations about Security and Human Rights*, CEPS Special Report, March 2009; Lindsay Aagaard, *A shared struggle for truth and accountability: Canada, Europe and investigations into the detention and abuse of citizens abroad*, CEPS Special Report, March 2009.

[3] Amandine Scherrer, *Good Practices as International Norms? The Modalities of the Global Fight against Transnational Organised Crime and Terrorism*, CEPS Special Report, March 2009.

been between the UK intelligence community and their US counterparts regarding personal data and information about Mr Mohammed during his captivity.[4]

The legal principle at stake in all these cases is the right to privacy and the right to data protection; two concepts that converge and diverge depending on the debate and the country in which they are under analysis. It is when the individual's right to privacy is superseded by the state's appreciation of a need to know about the person that problems arise. The confidence of state authorities in their counterparts in other states makes the sharing of this personal data among authorities and across borders a simple matter. In this paper I will not examine the issue of data sharing across borders between the public and private sectors, an issue at the heart of the SWIFT affair and also of the Passenger Name Record Agreements which the EU has entered into with Australia, Canada and the USA, and which permit authorities in those states to oblige private carriers in Europe to provide information about passengers to them.[5] I will focus instead on the difficulties inherent in the collection of personal data in the first place.

I will also look at some of the claims that people have brought before the courts in which the legitimacy of state action is under scrutiny. Notably the European Court of Human Rights decision in *S & Marper v UK*, where a supranational court finds the UK's maintenance of sensitive biometric data in its police database unlawful on the basis of privacy. Here the contention spills over the framework of democracy within sovereignty into the field of international human rights, where an individual is able to claim human rights against the state.

**Research questions:**

1. Where is privacy located?
2. Who defines privacy?
3. What are the principles of privacy?
4. What is necessary in a democratic society?
5. What is the role of supranational and national courts in determining the meaning of privacy and for whom?

## The challenges around privacy

The question of privacy rose to the top of the EU agenda at the beginning of 2010 for a number of reasons and from a number of sources. On the one hand, on 11 February 2010, the European Parliament rejected an interim agreement prepared by the EU Council and the US authorities that would have enabled agencies in the EU to continue to provide information to their US counterparts on all electronic bank transfers in Europe. The result was that the continued supply of this information to the US authorities was no longer lawful. The US authorities issued a press release expressing their disappointment and insisting on the importance of the information for anti-terrorism measures. The reason for the European Parliament's negative vote was the potential impact of the agreement on the privacy of EU citizens. The Parliament considered that the lack of satisfactory safeguards for the right to privacy made the proposed agreement unacceptable.

---

[4] Clive Stafford Smith, "Binyam Mohammed: A Shameful Cover-up" (http://www.guardian.co.uk/commentisfree/libertycentral/2010/feb/10/torture-guantanamo-bay).

[5] Peter Hobbing, *Tracing Terrorists: The EU-Canada Agreement in PNR Matters*, CEPS Special Report, September 2008.

On the other hand, the EU's own Data Retention Directive,[6] which requires telephone and internet operators to collect and store information on telephone, mobile phone and internet messages within the EU so that it can be available for law enforcement purposes, began to run into serious trouble in the national courts in the EU. Two member states, Ireland and Slovakia, asked the European Court of Justice (ECJ) in 2006 to annul the Directive on the grounds that there was a fundamental error regarding the legal basis. The ECJ refused to do so in a judgment in February 2009,[7] so the member states continued their rather tortuous national implementation of the measure. The Romanian Supreme Court found against the national implementing legislation in October 2009. Then the German Constitutional Court struck down its national implementing legislation on 2 March 2010.[8] In both cases it was the relationship of the intrusive nature of the legislation on the individual's right to privacy that was central to the decisions. The German court was particularly concerned about the purpose of the collection and storage of the data, which was precautionary in nature, that is to say not directed at events that had already taken place but at some future possible action or event. It found that retention of such data must not lead to the possibility to virtually reconstruct any activities of citizens. It found that it is a central element of Germany's constitution that citizens' activities in enjoyment of their rights and liberties cannot be subject to total capture and registration.

In the meantime, the European Court of Human Rights (ECtHR) has also been active on the question of privacy. On 4 December 2008, it handed down judgment against the UK regarding a law enforcement database that includes various items of biometric data on individuals.[9] It found that the blanket and indiscriminate nature of the powers of retention of fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences failed to strike a fair balance between the competing public and private interests, and that the UK had overstepped any acceptable margin of appreciation in this regard. Further, it found that the retention of the data constituted a disproportionate interference with the applicants' right to respect for a private life and could not be regarded as necessary in a democratic society (para 125). This is strong stuff indeed from an ECtHR that is sometimes criticised for mincing its words.

The contestation revealed by the events cited above is characterised first and foremost by a great curiosity by states to know more about people, both those living on their territory and farther afield, as the SWIFT affair indicates. All the issues relate to state authorities seeking more information about people, claiming a right to retain that information for periods it determines and to use the material in the future in ways not yet defined. In these cases, a common theme, as commented upon by the German court, is that the information is valuable in itself. State authorities are not seeking the information in order to find out who committed a crime. Rather they want the information stored and available for future use so that they can reconstruct the individual's activities virtually and follow him or her through databases that depict time and reveal events. Gary Marx has described this as the toast and freeze approach – information is toasted into a fixed form reflecting a specific moment, frozen in a database and when wanted, pulled out and toasted again. All the different bits of information may be toasted up and placed together, giving the impression of recreating the whole loaf of bread. But of course, it looks nothing like a loaf of bread – the processes through which the information has passed create a completely different data profile to the individual from whom they were first extracted.[10]

---

[6] Directive 2006/24, which had to be transposed into national law by 15 September 2007 – see the second part of this paper.

[7] C-301/06, *Ireland & Slovakia v European Parliament and Council*, 10 February 2009.

[8] http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-008.html

[9] *S & Marper v UK*, 4 December 2008 application, Nos 30562/04 and 30566/04.

[10] G. Marx, *Undercover: Police Surveillance in America*, University of California Press, LA, 1988.

Further, in the European context, the state's curiosity finds a new home in the European Union – the use of supranational measures to justify interferences which might be problematic to sell to home parliaments. The German court admonishes its national government suggesting that it must take the message to the European Union that precautionary and causeless data retention is by definition problematic for the right of privacy. However, just as the debate moves to the EU, the contestation does so as well. The European Parliament rejects the rather casual sharing of sensitive financial data of anyone with an active bank account in the EU with the US authorities with very limited and hard to enforce protections for the individual, but broad scope for sharing with US authorities and contractors. The European Court of Human Rights finds the UK authorities have overstepped the individual's right to privacy in retaining biometric data in a database. At the centre of the struggle are the research questions set out above. We will follow them through this study, trying to reveal the tensions and the solutions which the judicialisation of the right to privacy provides to them.

## *Where is privacy located?*

The constitutions of many EU states include a right to privacy. A right to both privacy and data protection is included in the EU's Charter of Fundamental Rights, which is now binding in all member states (with certain limitations in Poland and the UK).[11] This duty applies to the EU institutions and the member states' authorities equally. It is the judicialisation of the right to privacy that is of particular interest to us here. Who is entitled to determine the scope of the right to privacy or what is an unacceptable interference with it? What is the limit on the state authorities' claim to authority regarding the collection, retention and use of personal data? To answer these questions the relationship between state authorities and their national courts and supranational courts is central. They are charged respectively with the protection of the national constitution, including the delivery of constitutional rights to persons and protection European human rights contained in the ECHR. When faced with claims relating to privacy and data protection, the courts must decide whether the state's interest, which is based on a claim of responsibility for collective security, takes priority over the person's claim to privacy and the fair handling of his or her data in the name of individual security. For the 47 Council of Europe countries the building block of supranational privacy rights is Article 8 of the European Convention on Human Rights (ECHR).

Article 8 of the European Convention on Human Rights states:

> Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The right to privacy is one that finds a source outside national constitutional law in a regional human rights instrument. Of course, the ECHR is not the only regional or international human rights instrument to include a right to privacy. This can also be found, for instance, in the UN's International Covenant on Civil and Political Rights (ICCPR), but what makes the ECHR different as a source is the ECtHR. Unlike the ICCPR and other international human rights instruments, the existence of a court beyond the state that is charged with interpreting the instrument against the action of state parties changes the power relationship between the state and the individual. It takes the ultimate decision on what is privacy and whether it is being protected out of the control of state authorities, including national courts.

[11] Articles 7 and 8, EUCFR.

## *The facts of the Marper case*

The *Marper* judgment shows just how important the escape from the national jurisdiction and the authority of the state can be. In the case there are two applicants, Mr S who was arrested at the age of eleven and charged with attempted robbery. His fingerprints, cellular samples and DNA were taken. He was acquitted but his biometric data continued to be held in the UK's law enforcement database. The other applicant, Mr Marper, was arrested and charged with harassment of his partner. His fingerprints, cellular samples and DNA were also taken and added to the law enforcement database. Before even a pre-trial review, Mr Marper and his partner were reconciled and the charges were dropped. His biometric data were retained, however, in the database. The UK authorities refused to remove the biometric data from the database. The UK's Police National Computer, which contains the database, is governed by national law which is quite opaque and allows substantial discretion to the police. Their guidance provides for various degrees of access to personal data, easier access to that of persons convicted and more restricted for those who have not been. Time periods of retention range for 5 – 35 years, but the UK courts are not obliged to exclude data which should have been destroyed but was not, from being used as evidence in trials.[12]

## *Who defines privacy?*

The UK authorities stated that the retention of biometric data in a law enforcement database was not an interference with the right to respect for private life. The UK courts agreed with the UK authorities. Only at the final instance, in what is now the UK's Supreme Court, did one of the judges (Baroness Hale) suggest that actually retaining both fingerprints and DNA data constituted an interference by the state with a right to private life. Accordingly, a justification was needed for the action, and here the judge was fully satisfied that there was sufficient justification.

The ECtHR disagreed. It considered at length what 'private life' is according to its own jurisprudence. It found that there was not an exhaustive definition. By so doing, it allowed itself in the future to widen the meaning of the term should it consider this necessary. Thus the definition remains not only with the ECtHR but it remains an open question and one capable of being a site of further contestation. However, the ECtHR did find that private life can embrace multiple aspects of the person's physical and social identity. These include:

- Gender identification;
- Name;
- Sexual orientation;
- Sexual life;
- Personal identification and linking to a family;
- Health;
- Ethnic identity;
- Personal data revealing racial origin;
- Personal development;
- The establishing and developing of relationships with other human beings and the outside world;
- A person's image.

[12] *Attorney General's Reference (No 3 of 1999)*, [2001] 2 AC 91.

In light of such a wide range of issues held by the ECtHR to be part of private life, it is not surprising that it did not agree with the UK government or its courts about the question of whether retaining biometric data on a database is an interference with private life. It found that the mere storing of data relating to the private life of an individual amounts to an interference, within the meaning of Article 8 ECHR. This is independent of how the information might subsequently be used. The ECtHR found that all three categories of personal information – fingerprints, DNA profiles and cellular samples constitute personal data. Taking each category of data separately, the court examined its impact as regards the question of private life. Starting with cellular samples, it noted that it had already held that the systematic retention of this material constituted an interference with the right to a private life.[13] Although the UK government sought to change the ECtHR's mind on this, the attempt was not successful. The ECtHR, notwithstanding the opinion of the UK authorities, maintained its jurisprudence that in light of the highly personal nature of cellular samples their retention must be included as an aspect of privacy. Such samples could, for instance, reveal information about the individual including his or her health, it reasoned.

On DNA profiles, the ECtHR noted that less personal information was available from them than from cellular samples. Nonetheless, the ECtHR held that these too are part of private life because the substantial amounts of unique personal data which they obtain go well beyond neutral identification. It noted that DNA profiles can be used to establish family relationships and genetic links among people, thus their retention is indeed an interference with the right to private life.

As regards the third category of data, fingerprints, it was agreed that these hold less personal data than the other two. Here the ECtHR had previous case law of its own which indicated that holding fingerprint data is not an interference with private life. In an exceptional move, the ECtHR chose to change its jurisprudence on this point. It considered that fingerprint records constitute personal data in much the same way as personal photographs or voice samples. As in respect of the latter, the ECtHR has provided protection, in so far as it has held that fingerprint data should be brought into line:

> fingerprints objectively contain unique information about the individual concerned allowing his or her identification with precision in a wide range of circumstances. They are thus capable of affecting his or her private life and retention of this information without the consent of the individual concerned cannot be regarded as neutral or insignificant. (para. 84).

While it held that the retention of cellular samples and DNA profiles had a more important impact on private life than fingerprints, nonetheless, the retention of fingerprints constitutes an interference with the right to respect for private life. This means, for instance, that the EU's database of asylum seekers' fingerprints is caught by the new interpretation of Article 8 ECHR, as they are personal data.

Once the ECtHR has spoken there is no room left for the national authorities to argue. They are obliged to accept that it is the ECtHR that ultimately has the last word on what constitutes a private life. However, just because an element is constituted as part of private life does not mean that state authorities are prohibited from interfering with it. It simply means that the authorities must justify their interference. What changes is that instead of simply acting in respect of such elements as the state authorities consider best serves the public interest, the action has become interference. Thus they are obliged publically to justify why they are interfering with the elements that have become part of privacy. The justification must correspond to those permitted by Article 8 ECHR itself.

---

[13] *Van der Velden v The Netherlands*, No 29514/05 2006.

## *What are the principles of privacy?*

For an interference with privacy to be justified, it must first be in accordance with the law. But the definition of the law is once again a matter for the ECtHR, not the national authorities. So although national authorities may declare that they have a law that is adequate for the purpose of justifying an interference with the right to privacy, it is for the ECtHR to decide whether the legislation that the state puts forward fulfils the requirements of law according to the court's definition. Here the ECtHR reviewed its jurisprudence on what is law (thus identifying what is not law). The key feature of law is that is must be adequate and foreseeable. In other words, it must be formulated with sufficient precision to enable the individual to regulate his or her behaviour and conduct. To meet this threshold it must afford adequate legal protection against arbitrariness and indicate with sufficient clarity the scope of discretion of the authorities. Further, in so far as a margin of discretion is left to state authorities, the manner in which discretion is exercised must also exclude the arbitrary. The precision required from national law depends on the instrument under consideration, the field it covers and the number and status of the persons to whom it is directed. Once again, the ECtHR leaves itself substantial scope for defining what is law.

Regarding the UK's police computer, the ECtHR found that it is essential for law to fulfil the definition that in respect to the retention of personal data (specifically in the three categories which were under consideration in the case) it includes detailed rules governing the scope and applications of measures, as well as minimum safeguards including:

- Duration;
- Storage;
- Usage;
- Access by third parties;
- Procedures for preserving the integrity and confidentiality of data;
- Procedures for its destruction.

These safeguards are necessary to guarantee against the risk of abuse and arbitrariness. On the facts of the UK's case, the ECtHR did not make a finding as to whether the national law was entitled to be termed a 'law'. Instead it went on to consider whether there was a legitimate aim, since without a legitimate aim the interference with private life will never be justified. Here, however, the ECtHR has no trouble finding a legitimate aim: the detection, and therefore the prevention, of crime. There is an important temporal linking that the court carries out. The legitimacy is in the detection of crime and only via that route can it be for the prevention of crime. One has the impression that at least some voices in the court were perhaps concerned about the shift towards the detection of crimes which have not yet been committed or indeed might never be committed.

The taking of personal data from the individual, the court accepted, was for the purpose of linking the person to a particular crime where there is suspicion against him or her. The retention raises the rather delicate broader purpose of assisting in the identification of future offenders. The court does no more than mention, and then passes over, this aspect, which perhaps deserves much more attention. The reason for this is that the retention of data for the identification of future offenders means that one is reading backwards from the future an event that ineluctably will take place. Bigo calls this the "Future Perfect", an event in the future but for the purposes of the present justification has already happened.

### *What is necessary in a democratic society regarding privacy and surveillance?*

Next is the question of how the ECtHR deal with its relationship to democracy. This is unavoidable as Article 8 itself requires the court to reject any interference with privacy that is not justified as "necessary in a democratic society". The assessment of democratic necessity is expressly placed on the court's shoulders in the full knowledge that the 47 countries which are members of the Council of Europe are such because they have been accepted as democracies. The court begins by reminding us of the relationship of proportionality with democracy:

> an interference will be considered 'necessary in a democratic society' for a legitimate aim if it answers a 'pressing social need' and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are 'relevant and sufficient'.

This is quite a shopping list of elements to assess. While we have already dealt with the legitimate aim of the measure the court still invites consideration of:

- Pressing social need;
- Proportionality of the action in light of the aim;
- The relevance and sufficiency of the state authorities' justifications.

The final word on all of these counts will be the decision of the court, not that of the national authorities. However, the state authorities are, according to the court left what is called a 'margin of appreciation'. This margin will vary depending on factors which the court sets out (though they are not definitive):

- Whether the right at stake is crucial to individual's effective enjoyment of intimate or key rights;
- Whether a particularly important facet of an individual's existence or identity is at stake.

If either or both of these aspects are present then the state has a narrow margin of action. If they are not the state's action will be assessed against a wider margin of appreciation. In determining the two factors that widen or narrow the state's margin, the court indicates that what is central is the extent to which there is a consensus within the member states of the Council of Europe (all 47 of them). This will be both as regards the relative importance of the interest or how to protect it best. One way the court deals with the problem of contested democracy is through an assessment of what other states accepted as democratic by the Council of Europe do in respect of the same issues. However, to answer its questions, in the first place the court goes is to the ECHR itself. It repeats Article 8 which is, in its opinion, irrefutable evidence of the fundamental importance of the right to respect for privacy. Because Article 8 constitutes the consensus of democratic states, appropriate safeguards for the protection of personal data must be in place.

The next source of democratic legitimacy that the court uses is the Council of Europe's convention on automatic processing of personal data (1981). What it is effectively doing is maintaining that the other Council of Europe conventions relevant to the issue form a coherent part of the assessment of democratic legitimacy. This means that all the treaties of the Council of Europe form part of the basis for the assessment of democracy. The third step the court takes is beyond the treaties to the Recommendations of the Council of Europe's Committee of Ministers. It takes Recommendations R(87)15 and R(92)1 on the use of personal data in the police sector as evidence of the consensus of what is necessary in a democratic society in Europe. This provides more clarity on the safeguards that must be in place for data, specifically where it is sensitive, revealing, for instance, genetic make-up.

The ECtHR then refers back to its round-up, set out earlier in the judgment, of the law and practice in other Council of Europe member states and its comments regarding the inconsistency

of the rules within different parts of the UK. In that earlier section, it noted that 20 member states stored DNA information on national databases and the number is increasing. But it noted that in most of those countries the DNA information is not taken in a systematic manner but limited to specific circumstances and/or to more serious crimes (punishable by imprisonment). According to the ECtHR's study, only the UK expressly permits the systematic and indefinite retention of DNA profiles and cellular samples of persons who have been acquitted or in respect of whom criminal proceedings have been discontinued. Five states require such information to be destroyed on acquittal or discontinuance (Belgium, Hungary, Ireland, Italy and Sweden) while ten others allow for further retention only in most exceptional circumstances. At this point in the judgment the court also has regard to the EU rules on data protection (Directive 95/46) and the Prüm Convention of 2005 (entered into by some member states and then transformed into an EU Council Decision in 2008) which provide for time limits on the retention of personal data.

The message seems to be that democratic legitimacy can be assessed first, through the Council of Europe treaties and Committee of Ministers' Recommendations. Secondly, it will examine the practices in other Council of Europe countries. Thirdly, the inconsistencies within the state itself regarding data protection are a source of information regarding necessity in a democratic society.

The court then applies the agreed principles to the case. It accepts that the retention of fingerprints, cellular samples and DNA profiles may in general be regarded as justified within the ECHR. It limits its assessment to whether the retention of such information regarding people who have been suspected but not convicted of a criminal offence is justified. To do so it sets out the key principles of data protection:

- Proportionality to the purpose for collection;
- Limitations on periods of storage;

The court's justification for these two central planks is the Council of Europe Convention and the Committee of Ministers' Recommendations.

- The gravity of the crime and the existence of a conviction.

The justification here comes from norms across the Council of Europe states and the inconsistencies within the UK – Scotland has a system which is less oppressive and corresponds to the Committee of Ministers' Recommendation R(92)1. Although the court recognises the UK authorities' claim to the efficiency of having a large database, it uses against the UK its claim to be ground-breaking for the Council of Europe in this regard. If the UK claims such a position, according to the court, it carries a particularly heavy burden to ensure that private life is respected. The efficiency argument of the UK authorities is presented, in the judgment, as questionable on the basis of other academic work that casts some doubt on it. The court notes the authorities' own argument on efficiency is undermined by the fact that DNA samples taken from suspects are most matched with existing DNA profiles from earlier crimes, thus the temporal relationship is with past crimes and present suspects not present suspects and future crimes.

In finding against the UK authorities, the court specifically condemns two aspects of the UK's use of biometric data: the blanket nature of collection and the indiscriminate nature of retention. The catalogue of problems looks like this:

- Blanket and indiscriminate retention;
- No proportionality between offence and retention;
- No age limits;

- No time limit to retention irrespective of the offence;
- No scale of difference depending on the category of data engaged.

The ill the court identifies is that of stigmatisation. The retention of the data interferes with the presumption of innocence. This is because convicted and acquitted people are treated in the same way. While the court accepts that retention of data is not the same as the voicing of suspicions, the indefinite holding of data places them in the same category as the convicted person. These concerns are even stronger in relation to minors. The result is that the court finds:

> In conclusion, the Court finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society. This conclusion obviates the need for the Court to consider the applicants' criticism regarding the adequacy of certain particular safeguards, such as too broad an access to the personal data concerned and insufficient protection against the misuse or abuse of such data.

## Conclusions

The Stockholm Programme, the new five-year plan for the development of the Justice and Home Affairs area, requests that the Commission

> explore if and how authorities of one Member State could obtain information rapidly from private or public authorities of another Member State without use of coercive measures or by using judicial authorities of the other Member State.[14]

Similarly, it calls on the Commission to

> examine how operational police cooperation could be stepped up, for example as regards incompatibility of communications systems and other equipment, use of undercover agents, and, where necessary, draw operational conclusions to this end.[15]

In carrying out these activities, the Commission will have regard to the ECtHR jurisprudence and ensure that its actions do not encourage or attempt to justify breaches of the individual's right to privacy through exchange of fingerprints, cellular samples of DNA among law enforcement authorities where even the retention of such samples is contrary to the ECHR. This is even more important when it comes to the transfer of data from the authorities of one state to another – the obligation to ensure that there are satisfactory controls over what data is being shared with whom and for what purposes is critical.

Finally, the Lisbon Treaty has made the EU Charter of Fundamental Rights legally binding and of equivalent status to the EU treaties themselves. The Charter contains at Articles 7 and 8 both a right to respect for private and family life equivalent to Article 8 ECHR (in respect of which the UK came unstuck in *S & Marper*) and a right to the protection of personal data. People in the EU now have a right not only to privacy but also to protection of their data, which includes protection from its too casual transmission to the authorities of other countries.

[14] Stockholm Programme, Council Doc 5731/10, 3 March 2010, .p 40.

[15] Ibid., p. 69.