Legally compatible Design of future biometric Systems for Crime Prevention

Matthias Pocs[1]

Universität Kassel, Kassel, Germany

Innovations in emerging technologies have an impact on privacy and fundamental rights. For example emerging technologies are future biometric systems for crime prevention. In contrast to large-scale biometric systems for migration control (Karyotis 2007), these systems promise to track down terrorists and organized criminals but also entail novel risks for society. One can govern science and technology by means of privacy impact assessments (which are currently being researched (Friedewald *et al.* 2010) (SAPIENT 2011)). Alternatively there is the approach - used in this paper - that primarily builds on the assumption: Technology design can render the violation of a legal norm impossible. Using German and European constitutional law as an example, this paper will present proposals for technology design derived from the law.

Keywords: privacy by design; privacy impact assessment; data protection law; fundamental rights; security technologies.

1. Introduction

At the airport the police scan fingerprint traces left on luggage before boarding. Should a terrorist cause the aircraft to crash, the data captured in the beginning are searched on already known data from a database of criminals. This is one example of possible future crime prevention scenarios where biometric data play a significant role. Already now, police authorities have tested and used biometric technology (Bundeskriminalamt 2007) (Gates 2010) (Thomas 1998) (Daugman *et al.* 2004) and respective research is funded (Hildebrandt *et al.* 2011) (Bouchrika *et al.* 2011).

Due to this development it is possible that legislators will allow the police to use biometric systems in public places for preventing terrorism, organized and crossborder crime. In this scenario one captures data before knowing that the person checked is a criminal or before a crime is committed. Such a precautionary data capture challenges the law (Desoi *et al.* 2011) (Pocs 2011a) (Hildebrandt *et al.* 2011) (Hornung *et al.* 2010). Particularly this is because one captures biometric characteristics without the individual having given cause for it, as well as a large number of persons is subject to it.

One can avoid several risks to individuals' freedoms and society's democracy by means of technology design. This paper will present proposals for technology design derived from the law. It uses German and European constitutional and data protection

[1] Email: mp@matthiaspocs.de

law as an example for the law. For the technology it uses future biometric systems for crime prevention as an example. The paper aims at engaging in the discussion around the impact of innovations in emerging technologies on privacy. It also tries to contribute to the development of new instruments for the governance of science and technology.

2. Future biometrics and its opportunities and risks

In future biometric systems for crime prevention nonsuspects are exposed to specific risks. In order to derive proposals for technology design from the law, one needs to know the special features of that technology as well as its risks to privacy.

2.1 Biometric scenarios for crime prevention

The deployment of future biometric systems for crime prevention challenges the law because it differs from deployment of conventional systems for biometric access and ID card checks. This is particularly because they capture biometric characteristics by automatic means in uncontrolled environments where the individuals do not have to cooperate and hence cannot control the data capture.

This paper presupposes two scenarios at the airport. One scenario is biometric data retention for use in case that an incident occurs during the flight; another scenario is biometric data capture for instant comparison with wanted lists. In the first scenario, before the take-off of an aircraft all fingerprint traces that are left on luggage are captured and stored as a precaution for crime prevention (see (Hildebrandt *et al.* 2011) no. 5.2). However, due to the design one can only use the data of a flight if a trusted third party such as a data protection authority cooperates (Pocs 2012a) (Pocs 2012b). If then a predefined incident occurs (airplane crash, hijacking, members of criminal networks travelling or similar), the police can use data to identify known criminals involved.

In the second scenario, facial data (with fingerprint traces this is not possible now) are captured from CCTV cameras and instantly compared to wanted lists. Both scenarios aim at affording the police clues for detecting criminal networks and in addition, the second scenario aims at detecting and stopping criminals on the spot.

2.2 Opportunities and risks of the technology

For society, the deployment of future biometric systems affords opportunities and entails risks. On the one hand the deployment could prevent crime. On the other it entails specific risks (Desoi *et al.* 2011) (Pocs 2011a) (Hildebrandt *et al.* 2011) (Hornung *et al.* 2010):

- Revealing sensitive information from biometric raw and template data (Working Party 2003, no. 3.7),
- Connecting several databases to create a personality profile due to biometric characteristics' uniqueness,
- … universality (everyone has biometric characteristics) and
- … life-long validity,
- Gaining information about whereabouts, time and destination,
- "False hits,"

- Secretive data capture (fingerprints and faces leave traces (Working Party 2003, no. 3.2),
- Unauthorized data access ("identity theft"),
- Function creep of data access (e.g. punishment of minor offences or creation of profiles about witnesses, contact persons, etc. (in detail (Pocs 2011a)), as well as
- Follow-up measures by the police on the spot of system deployment.

In the future, legislators could allow the police to use systems that automatically capture biometric characteristics and compare them with wanted lists. Then one has to fear that the deployment cannot be checked because the technology affords unlimited possibilities of social control. This paper analyses the impact of technology on privacy and the way to govern science and technology by means of technology design.

3 Legality of future biometrics

Future biometric systems have to meet requirements from national constitutions like the German *Grundgesetz* (GG) and European Convention on Human Rights, and EU Treaties and Fundamental Rights Charter.

First, one has to consider the fundemental rights to informational self-determination (Germany), privacy and data protection (EU). In addition human dignity could be concerned if state authorities use biometric characteristics as single identifiers for treatment of data subjects as mere "objects." Moreover, the special protection of sensitive data (Article 8 DPD) such as health and ethnic information could be applicable at least to some forms of biometric data. Besides the right to travel and the freedom of movement could be at risk in case that the police track and continuously monitors individuals in different places.

Finally several other fundamental rights could be violated: property and free movement/freedom to travel (in case of confiscation); assumption of innocence and equality (if the system or its design suffer from errors); judicial review (in non-transparent systems); and prohibition of arbitration (in case of unspecified purpose of use) (Hornung *et al.* 2010).

3.1 Governing science and technology by legal technology design

One can govern science and technology by privacy impact assessments. These are currently being researched in general (Friedewald *et al.* 2010) and particularly with a view to smart surveillance technologies (SAPIENT 2011). Another similar method is to "regulate" the technology design.

However one should bear in mind that technology design does not replace the law but it can render the violation of a legal norm impossible. The relevant legal norm necessarily precedes the technological design. Therefore one does not make the prohibition of unlawful data processing redundant but instead enforces it by technology design. There are a number of implications in such technological enforcement, which have been discussed extensively (see e.g. (Brownsword 2006) and (Citron 2007)). It is questioned whether technology design can still be referred to as "law" (Brownsword 2006). It is also pointed out that automated implementation of legal rules should contain specific safeguards to guarantee, amongst other things, transparency (Citron 2007). In consequence, one cannot necessarily assume that design replaces a legal prohibition, but

it is clear that it can enforce preceding constitutional legal norms which legitimize the design.

In order to regulate technology design, one can derive specific requirements for information and communication technology systems from legal rules. One example of such legal technology design is described is already described (Hammer *et al.* 1993). Legal technology design also promotes the principle of "Privacy by Design" (Pocs 2012c) which in the future will be part of EU law (see 3.3.4). The following section will identify legal requirements for the design of future biometric systems for crime prevention.

3.2 Constitutional requirements in Germany

Laws permitting police to use biometric surveillance systems have to meet German constitutional requirements. In its case law the Bundesverfassungsgericht (Federal Constitutional Court of Germany) specified the these requirements.

3.2.1 Anonymisation

The legal provision that allows the police to use the system deployment has an impact on the fundamental right to informational self-determination according to Article 2(1) together with Art. 1(1) *Grundgesetz*. This is because the future biometric system processes biometric data and criminal records .These are personal data within the meaning of § 3 of the German Federal Data Protection Act (*Bundesdatenschutzgesetz*) and Art. 2(a) together with Recital 26 of the EU Data Protection Directive 95/46/EC (DPD). From this, one can also derive the first legal criterion, that is, designing the system in a way that avoids identifiability by anonymizing or pseudonymizing biometric data (Desoi *et al.* 2011).

3.2.2 Precision of the legal basis

The legal basis permitting the biometric system must specify, precisely and clearly, the "cause" ("*Anlass*"), purpose and limits of system deployment (Bundesverfassungsgericht 2008, p. 424). For police measures, legislators need to define a specific suspicion or danger as a requirement (Bundesverfassungsgericht 2004, p. 55). They can do this by limiting (1) the wanted lists, (2) data capture, and (3) subsequent use of information. One has to regard the interplay of these three components in order to assess proportionality (Bundesverfassungsgericht 2008, p. 432).

First, legislators have to specify conditions for the inclusion into the databases for comparison, that is, the wanted lists. One needs to distinguish suspects and nonsuspects (witnesses, contact persons, etc.), facts and mere assumptions, etc. From this, one can derive another legal criterion of technology design. One should design the system in a way that enables the police to distinguish between data subjects according to these conditions for the inclusion into the wanted list (Pocs 2011a).

Second, legislators need to define conditions for the data capture. This includes the place of system deployment (airport, football stadium, shopping mall, school or similar). Third legislators need to limit the subsequent information use (courts must not use "hits" as evidence for a crime (Pocs 2012a)).

Further, legislators must specify the technology design in a qualified, at least basic, precise and binding manner (Bundesverfassungsgericht 2010, p. 225). Hence legislators can define certain goals that the technology design must achieve.

3.2.3 Suitability and necessity

The technology deployment needs to be suitable and necessary for achieving its goal. At least, the system deployment does not evidently prove to be unsuitable if the data captures could be successful in certain cases (Bundesverfassungsgericht 2009). This is very controversial and requires serious scrutiny. Therefore one should not understand technology design as legitimizing biometric systems that do not achieve the stated purpose.

In this case, the biometric system aims at aiding the police in detecting criminal networks. This means that the wanted list must only contain known persons that are suspects based on facts according to conventional constitutional police laws. Persons that match certain profiles based on statistical inferences (e.g. (Harcourt 2007) and (NRC 2008)) must not. The distinction by the police between suspects and nonsuspects as well as the facts and mere assumptions is crucial (see Section 3.2.2).

Further, not only false positives or "false hits" stigmatize individuals. Rather, the mere fact of a match is problematic. This is because the match solely confirms that one belongs to a certain category that might – based on other evidence – be involved in criminal action. Therefore, a match or a "hit" must not imply being guilty. Police and courts must not treat innocent people as criminals. This is even true if the hit is not a false hit because the very inclusion of a person in a wanted list could be erroneous too. If respective safeguards are not in place, the system deployment is ineffective and thus unsuitable for achieving the stated purpose.

Legislators have to show that using the biometric system, police can in fact detect organized crime and terrorism. It is not enough to present facts that sound plausible. Rather one needs to conduct an empirical study. This study has to stand the test of the latest state of the art of criminology and application of its methods.

Apart from suitability, the system deployment is only necessary if no less intrusive and equally effective means is available. One has to take into account all biometric modalities (iris, fingerprint, face, gait, etc.). "Nontraceable" modalities (gait/iris) are less intrusive than modalities with which one leaves traces in many circumstances of daily life (CNIL 2007). Capture of fingerprints and faces also harms the effectiveness of existing biometric systems used for forensics, secret service, and witness protection (Pfitzmann 2006).

3.2.4 Proportionality (in the strict sense)

Finally one must balance the impact on individuals and the goals pursued with the system deployment. One assesses the proportionality (in the strict sense) of automated capture of personal data by using several criteria.

Detecting criminals. The goals of the system deployment specified in the legal basis are to detect criminal networks and individual criminals. In the case of future biometrics the purpose will have to be limited. The group of wanted persons should be small, that is, only for very serious crimes and a large content of wrongdoing. Then the goals pursued by the system deployment are serious.

Public nature. The biometric system captures data in a public place. Accordingly everybody can see or otherwise perceive the biometric characteristics. The public nature reduces the impact on individuals according to the *Bundesverfassungsgericht* (Bundesverfassungsgericht 2008, p. 404).

However, one can argue against this legal criterion. "Privacy in public" is an important value because precisely the anonymity of the crowd provides an individual with privacy (Nissenbaum 1997). Biometric systems could identify individuals and thus violate this expectation of privacy or render superfluous the legal criterion of the public nature. Moreover the biometric machine/software "perceives" biometric characteristics in an entirely different manner than human beings. Therefore, it is not relevant that police use the system in the public. This is because the software can store the data and render them searchable (inferring information not available to the naked human eye).

Data collection as mere aid. Police only deploy the biometric system in order to look for people already known and have given cause for suspicion/danger. The system processes data about a large number of innocent people but only temporarily and deletes them automatically. Hence, the technology use is merely an aid to identify persons and immediately take police measures (Bundesverfassungsgericht 2008, p. 404). This reduces the impact on individuals. However the following criteria will assert that the impact on individuals is higher.

Lack of cause. The system deployment lacks cause if neither a danger for certain objects of legal protection nor a suspicion of having committed a crime justifies the system deployment (Bundesverfassungsgericht 2008, p. 402). For such an indiscriminate data capture, the individual has not given cause.

"High scatter." Further, the system deployment involves a so-called high "scatter" of data processing (or a "serious collateral intrusion into privacy"). This is because a large number of persons that have not given cause for the data collection are subject to it (Bundesverfassungsgericht 2008, p. 402). From this, one can also derive the legal criterion to design the system in a way that avoids a high scatter of captures and comparisons of biometric data.

Feeling like being watched. The system deployment could provoke the feeling of being watched. Such a feeling can be a consequence of the high scatter of the data processing (Bundesverfassungsgericht 2008, p. 403). As an argument from the contrary, this means that avoiding a high scatter also promotes the criterion of avoiding the feeling of being watched.

Adapting behaviour. Further the system deployment could lead to individuals adapting their behaviour which functionally corresponds to impacts on other fundamental rights of the data subjects (Bundesverfassungsgericht 2008, p. 406).

Transparency. The system deployment might violate the principle of transparency. "Transparency" refers to two concepts. On the one hand, legal protection is hampered if individuals do not know enough about the technology use (Bundesverfassungsgericht 2008, p. 403). In contrast to video surveillance, it is not only relevant to know about the camera but also about matches or "hits" (Bundesverfassungsgericht 2008, p. 406).

On the other hand, transparency can be systemic. Legislators can achieve such a system transparency by involving data protection authorities. Hence the legislator of the European Community did this in Arts. 18, 20, 22 and 28(3) of the DPD. It is typical for police measures for searching wanted persons that transparency for the individuals and the access rights have to be limited; therefore the constitution requires the checking by completely independent state authorities (Bundesverfassungsgericht 2001, p. 361). System transparency is particularly relevant due to the secretive nature of police measures and the "high scatter" of the future biometric system for crime prevention. From this, one can also derive the legal criterion to design the system in a way that avoids identifiability and processing if the data protection authority does not cooperate.

Data minimisation. In Germany the principle of "data avoidance and data frugality" according to § 3a BDSG is recognized on the constitutional level (Bundesverfassungsgericht 2010, p. 270). It requires designing the technology with the goal of processing only as little personal data as possible. If the biometric system does not use anonymisation technologies (e.g. "Biometric Template Protection"), the principles are violated and the impact on individuals is more serious.

Use limitation. The principle of use limitation prohibits using personal data for other purposes than originally specified (Bundesverfassungsgericht 1983, p. 65). In the case of future biometrics one cannot rule out the possibility that legislators later enact a law that permits data access for other purposes. Thus the impact on individuals is more serious. One can also derive the design criteria such as designing the biometric system in a decentralized way that avoids concentration of informational power.

Data security. For the system deployment legislators need to safeguard a standard of data security that takes the specific impact on individuals into account (Bundesverfassungsgericht 2010, p. 224). Depending on the technology design, the police might violate this principle.

Stigmatization. The impact on individuals is more serious if the data subject is put under pressure to offer an explanation (Bundesverfassungsgericht 2010, p. 212) or is stigmatized (Bundesverfassungsgericht 2005, p. 351). Biometric (one-to-many) identification systems are subject to specific error rates (TeleTrust 2006, p. 15). Individuals could therefore be subject to "false hits" which stigmatizes her/him. Hence the impact on individuals is more serious.

Uniform personal identifiers. Another requirement follows from human dignity according to Art. 1(1) *Grundgesetz*: one must not use uniform personal identifiers for comprehensive registration of the data subject (personality profile) (Bundesverfassungsgericht 1983, p. 53). Certainly the police would not deploy the biometric system for comprehensive registration. However due to their uniqueness, universality and life-long validity, biometric characteristics could be used accordingly and thus render the impact on individuals more serious.

3.3 Constitutional requirements in Europe

Laws permitting police measures using biometric surveillance systems have to meet European constitutional requirements. In Europe Art. 8 European Convention on Human Rights protects privacy and Arts. 7 and 8 EU Fundamental Rights Charter

protect privacy and data protection. The legal basis for data protection law is enshrined in Art. 16 of the Functioning of the EU Treaty. This means that the EU will pass secondary law for data protection in the area of police and criminal justice (Commission 2012a).

This paper regards German and EU law as two parallel legal systems and uses both for deriving technology design proposals. This approach is due to a certain rationale. According to the European Court of Justice, EU law also takes precedence over the constitutional law of Germany (*Internationale Handelsgesellschaft* C-11/70 (1970) ECR 1125; *Costa v ENEL* 6/64 (1964) ECR 585). In contrast, the Bundesverfassungsgericht first did not accept this view. This was because the EU had no legal protection that would satisfy the German standard of fundamental rights (Bundesverfassungsgericht 1974, p. 285). Later this changed since the court held that it would normally not review the compatibility of secondary EU law with fundamental rights (Bundesverfassungsgericht 1986, p. 387). However the court regards the German fundamental rights as being also applicable to EU law and thus reserves the right to have the last word in exceptional cases (Bundesverfassungsgericht 1993, p. 175).

3.3.1 ECtHR case law

Before the coming into force of the Treaty of Lisbon in 2009, provisions for privacy and data protection in police and criminal justice were missing in EU primary law. Instead, the Council of Europe was in charge for fundamental rights according to the European Convention of Human Rights. The ECHR provides for privacy protection in its Art. 8 which is also the basis for the Data Protection Directive 95/46/EC (DPD) in line with Rec. 46 DPD.

The ECHR is interpreted by the European Court of Human Rights (ECtHR). Its case law gives guidance for the privacy protection in police measures. Further, the Council of Europe adopted a recommendation for the police sector (Recommendation (87)15) which however was not often considered (Bygrave 1998, p. 265).

Introduction. In general, privacy/"private life" has a broad ambit which extends beyond domestic sphere (*Peck v. UK* 2003). Similar to German constitutional law, the court examines impact on privacy according to Art. 8(1) using several criteria such as: storage of personal data (*Amman v. Switzerland* 2000), consent and awareness, nature of the information, and re-purposing of the information.

According to Art. 8(2), the legal authority needs to promote a legitimate aim referred to in that provision, be necessary for achieving that aim, and specify the purpose. The legal authority is necessary if it answers a "pressing social need" and is "proportionate to the legitimate aim pursued." The purpose specification must be sufficiently precise and clear for individuals to foresee the technology deployment (*Kruslin v. France* 1990, para. 33; *Malone v. UK* 1984, para. 68).

Foreseeability. Regarding foreseeability, the ECtHR reaffirmed that the requirement of specifying the scope and manner of technology deployment also applies to police measures (such as phone interception) (*Liberty v. UK* 2008; see also Nos. 2(1) and 5(1) Recommendation R(87)15).

However, it also acknowledges that the requirement of foreseeability cannot be "the same in the special context of interception of communications for the purposes of police investigations." This was because "the object of the relevant law is to place restrictions on the conduct of individuals." In particular, an individual should not

"foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly" (*Malone v. UK* 1984, para. 67). Nonetheless, the law needs to provide for the category of individuals exposed to the surveillance, its circumstances, and the conditions for destroying recordings (*Kopp v Switzerland* 1998, paras. 73–75; *Kruslin v. France* 1990 A 176-A, para. 35; *Huvig v. France* 1990 A 176-B, para. 34).

Necessity. Regarding the necessity of police powers, the ECtHR only accepts powers of secret surveillance of citizens "only insofar as strictly necessary for safeguarding the democratic institutions" (*Klass v. Germany* 1978, para. 42). Unlike in Germany, "necessary" also means "proportionate." In particular, it is disproportionate to store (DNA) data about non-convicted individuals. Even if the police would collect the data for a good reason they need to delete these data as soon as the individual turns out to be innocent. It is unlawful to retain data for the sake of preventing future committal of crimes where most individuals will not commit a crime (*S and Marper v. UK* 2008). This resembles the Bundesverfassungsgericht's criterion of indiscriminate data processing and high "scatter" of data processing mentioned above.

In contrast to the German constitution, the term necessity is however broader in the ECHR. In Germany, the suitability and necessity only refers to the introduction of a police measure as a whole. The technology design and its impact on fundamental rights is evaluated no sooner than during the assessment of proportionality in the strict sense. However, the ECtHR understands that "necessity in a democratic society" includes both a "pressing social need" (this is similar the German notion of necessity) and proportionality. Therefore, it seems that these legal principles are not as strictly distinguished as in Germany.

Accordingly, the necessity requires serious scrutiny, especially since the use of biometric system for the fight against crime is very controversial. As mentioned above, one should not understand technology design as legitimizing biometric systems that do not achieve the stated purpose. Rather, the use of the biometric system must be effective and meet the requirements mentioned in that regard (see Section 3.2.3). Otherwise, the system deployment is ineffective and thus prohibited by the ECHR.

Transparency. Since it is typical for police measures that transparency for the individuals is limited, also the ECtHR acknowledges the checking by completely independent state authorities (*Kruslin v. France*, para. 30).

Positive obligations. Privacy protection also entails "positive obligations" on the state, for example, to provide for IT security measures (*I v. Finland* 2008), access rights (*Von Hannover v. Germany* 2004; *McGinley & Egan v. UK* 1998; *Guerra v. Italy* 1998; *McMichael v. UK* 1995; *Gaskin v. UK* 1989) and rectification rights (*B v. France* 1992; *Cossey v. UK* 1990; *Rees v. UK* 1986).

Sensitive information. The ECtHR also recognises the need to specially protect sensitive information. It holds that these are data which "call for the most careful scrutiny on the part of the Court, as do the safeguards designed to secure an effective protection" (*Z v. Finland* 1997, para. 96; see also Art. 6 Convention 1981 ETS no. 108). Since from biometric data one can also obtain data about health and ethnic origin, this special protection is relevant.

Reasonable expectation. An additional criterion is the reasonable expectations of individuals (*Copland v. UK* 2007; *Halford v. UK* 1995) which reminds of the US

approach. However unlike the US courts, the ECtHR does not rule out an impact on privacy solely based on this criterion; it only influences the impact on individuals.

Comparison with the Bundesverfassungsgericht and EU Directive. Legal protection by the ECtHR can be weaker in some instances than that of the *Bundesverfassungsgericht*. First, the legal authority does not have to be a legislative authority. It can also be a merely ministerial order. Further, the doctrine of "margin of appreciation" leaves European states room for manoeuvre with respect to the proportionality assessment, extent of the state's positive obligations, and establishment of facts. However several aspects narrow the margin of appreciation: the importance of the right concerned, the impact on individuals, the purpose of system deployment, and extent of common European standards (*S and Marper v. UK* 2008).

Moreover, it is weaker than the EU Directive is in relation to transparency. Transparency could follow from the requirement of effective remedy for the individual pursuant to Art. 13 ECHR. However the Court holds that it is incompatible with the efficacy and purpose of surveillance if the police would have to notify individuals, even if only after the surveillance (*Leander* 1987 A 116, para. 66; *Klass* 1978 A 28, para. 58). The ECtHR offers less legal certainty in two regards. It is unclear what information use is covered by the right to privacy and how it influences the impact on individuals (*"somewhat confusing"* (Bygrave 1998, p. 263)). It also offers a lower standard of protection (*"hurdles not difficult to jump"* (Bygrave 1998, 268f.)).

Overlap with the ECJ. Sometimes the ECJ also decided on matters that fall within police and criminal justice. In particular, this competence is due to the discrimination between EU nationals. Particularly EU countries it prohibited national centralised databases for the fight against crime if they do not store data about nationals but only about people from other EU countries. The fight against crime necessarily involves the prosecution of crimes and offences committed irrespective of nationality. Therefore the situation of a Member State's nationals cannot be different in relation to this objective from that of non-national EU citizens (*Huber v. Germany* C-524/06, 16.12.2008, paras. 78f.).

3.3.2 European Union law

In the future, it is the EU which will govern data protection for police and criminal justice. The ECtHR's case law will remain to delineate the minimum level of protection. This is due to the recognition of the so-called "general principles" including the ECHR according to Art. 6(3) TEU (codifying (*Carpenter* C-60/00 (2002) ECR I-6279; *Nold* C-4/73 (1974) ECR 491, para. 13.)).

Moreover, since 2010 the EU has the power to accede to the ECHR according to Protocol No. 14 ECHR (amending ETS no. 194). As soon as the EU has acceded, the ECtHR could have the last word. This is the case if Art. 8 ECHR and Art. 8 FRC are equivalent (Streinz 2011, p. 604). According to Art. 52(3) FRC, provisions of the ECHR and EU FRC have the same meaning and scope insofar as they are equivalent. However, insofar as EU law offers a higher level of protection, the ECtHR will not restrict privacy and data protection. This is because Art. 52(3) FRC only harmonises the ECHR and FRC as a minimum level of protection.

Since the EU will govern data protection for police and criminal justice, the European Court of Justice is competent. Judicial review by the ECJ could prove beneficial to privacy and data protection in the police sector because in contrast to the

ECtHR, the ECJ applies additional legal mechanisms. These mechanisms include primacy of EU law (since *Costa v. ENEL* 6/64 (1964) ECR 585), direct effect (for the Treaty since *Van Gend en Loos* 26/62 (1963) ECR 1; and for directives since *Van Duyn* 41/74 (1974) ECR 1337), state liability (since *Francovich and Bonifaci* C-6/90 and C-9/90 (1991) ECR I-5357), equivalence and practical possibility (*Comet BV v. Produktschap* C-45/76 (1976) ECR 2043) and effectiveness (since *Factortame I* C-213/89 (1990) ECR I-2433).

3.3.3 Secondary law of the European Union

The EU will govern police data protection by means of specific secondary law. The future Police and Criminal Justice Data Protection Directive (Commission 2012a) will provide for specific rules in the police sector. The current data protection law of the EU will inspire it. However it will also provide for new rules. It will introduce new principles (Arts. 4 to 11), create and restrict notification of data subjects (Arts. 13, 15, 16 and 18), and introduce data breach notification (Arts. 28 and 29). Moreover it will give to the data protection authority's stronger powers and stricter duties (Arts. 18 and 46), and create remedies and compensation for individuals and bodies (Arts. 50 to 52).

System transparency. The biometric system must be transparent (see Section 3.2.4). Legislators can achieve such a system transparency by involving data protection authorities. Hence data protection authorities are involved in a way that is stricter than requirements from German law because the data protection authority needs to be "completely independent" (C-518/07, 9.3.2010). This is particularly relevant for surveillance measures. In order for the data protection authority to not only be independent from the police authority but also from the ministry of the interior which influences the police work.

Sensitive data. Sensitive data are data about ethnicity, health, etc. (Art. 8 (1) DPD), and data about criminal records or similar (Art. 8 (5) DPD). Thus the biometric system could process sensitive data because from biometric data one can extract ethnic and health data (Working Party 2003, no. 3.7) and any crime prevention system processes criminal data. This also entails the technology design criterion to separate sensitive data from the captured biometric data and delete them.

Data accuracy. Due to the abovementioned error rates, the system deployment could violate the principle of data accuracy according to Art. 6(1)(d) DPD.

Automated decisions. Further, due to the abovementioned error rates, the system deployment could violate the prohibition of automated individual decisions according to Art. 15. In relation to the principles of data accuracy and the prohibition of automated individual decision, one can also derive another legal criterion of technology design. One should design the system in a way that ensures compliance with an upper limit of false "hits."

3.3.4 In particular: Privacy by Design and similar provisions

Privacy by Design. The principle of Privacy by Design requires taking appropriate technical and organisational measures at the planning stage so as to comply with the

data protection provisions (Working Party 2009) (see also Art. 19 of the future Directive (Commission 2012a)). The principle requires governing science and technology by means of technological design which constitutes the theme of this paper. All design criteria mentioned in this paper promote the principle of Privacy by Design.

According to Art. 23(4) of the future general regulation (Commission 2012b) the Commission could even implement the principle of Privacy by Design by means of specific technical standardisation. Similarly there have been first attempts of the EU Commission to implement the principle of Privacy by Design. One example is the RFID PIA Framework (Working Party 2011a). The goal of this Framework was to develop "guidance for the design of RFID applications in a lawful as well as socially and politically acceptable way" (Commission 2009).

Another example of a tool for Privacy by Design is the EU Commission's pursuit of best practices for two associations in the field of online behavioural advertisement. They aim at specifying the opt-out rule in Art. 5(3) of the ePrivacy Directive 2002/58/EC (as amended by Directive 2009/136/EC). In particular the best practices provide for the design of cookies (Working Party 2011b).

The PIA Framework and best practices are only first attempts to implement Privacy by Design and in need of improvement. To this end this author proposes to adopt two additional rules: 1) a certain report demonstrating how a certain technology design promotes fundamental rights and 2) a five-step procedure for the interdisciplinary cooperation between lawyers and technologists (Pocs 2012).

Accountability. The principle of accountability requires technology users to be able to demonstrate that they have chosen and adjusted a legally compatible technology (Working Party 2010, para. 34) (see also Art. 18 of the future Directive (Commission 2012a)). The demonstration adds to Art. 5(2) of the current DPD which only requires "ensuring" compliance.

Accountability enforces Privacy by Design in three steps. Compliance rests with the Privacy by Design requirement. Consistently one has to audit if appropriate the fact that one has taken the required design measures. Then one has to be able to demonstrate this. This is why one needs to retain the audit report for the supervisory authority. If one does not comply with one of these steps, according to the Commission, the supervisory authority would be able to impose a dissuasive fine on controllers.

Since Accountability enables the police and others to demonstrate technology design some also regard Privacy by Design as a part of Accountability (European Data Protection Supervisor 2010, p. 105). Due to Accountability it is possible to demonstrate that one chose and adjusted the technology in a legally compliant way.

Privacy Impact Assessments. Privacy Impact Assessments will be mandatory for use of technology that entails specific risks for privacy and data protection. One can enforce Privacy by Design with PIA in two steps. It obliges technology users to assess in advance specific risks for "rights and freedoms" of data subjects that are entailed by a planned data processing process. Then they have to take measures to mitigate those risks (Clarke 2009). In particular, biometrics is set as a technology that requires the carrying out of PIA (Art. 33 of the future General Regulation (Commission 2012b)).

PIA adds to the prior checking according to Art. 20 of the current DPD because it provides for a legal compatibility test. It takes not only data protection into account but moreover the "rights and freedoms" of individuals as a yardstick for the assessment. That is, instead of a legal compliance test, there is a legal compatibility test within the norms of the EU Fundamental Rights Charter. Taking fundamental rights as a starting

point is sensible because in relation to novel technology applications EU secondary law is full of gaps in the description of technology design.

3.4 Summary

To sum up it is apparent that future biometric systems for crime prevention have a large impact on the fundamental rights to privacy and data protection. If the police render crime prevention effective by means of automated capture of biometric data, they need to do this for the protection of fundamental rights too. They should use automatic means to protect those who are subject to the data capture or (false) "hits" and possible follow-up measures by the police. That is, just as the goal of crime prevention, police need to use automatic means to reduce the risks for individuals and society.

Further, if the police process personal data prior to criminal activity, they should also ensure transparency and supervision prior to violations of privacy and data protection. This too suggests the development of technological measures for Privacy by Design, Accountability and Privacy Impact Assessments as well as legally compatible technology design. The law needs to define these technical measures to satisfy the necessary precision of the legal provision.

4 Examples of design proposals for future biometric systems

Supporting the abovementioned legal requirements and design criteria, one can only be realize legally compatible technology design together with developers, operators, and users. Since the research on the biometric system for crime prevention is work in progress, the following part will present a selection of such design goals they have identified so far.

There are simple measures to reduce the impact on individuals. For example, the system could reduce the number of data captures to random data captures (Bundesverfassungsgericht 2008, p. 430). However there are also more sophisticated elements of legal technology design. The following section will present them.

4.1 Coarse scans (based on (Hildebrandt et al. 2012))

The mere fact that a fingerprint trace is at a certain position on luggage scanned can indicate suspicion or danger if it was not located there before checking in the luggage. For example, in variation of the scenarios (see Section 2.1), the police use such indication in the following scenario: During luggage handling at the airport, the scanner captures all fingerprint traces on bags, once before luggage handling and once afterwards. Then, the system only compares the numbers of the fingerprint traces. If there are more traces afterwards there is reason to believe that someone manipulated the luggage in the security zone of the airport. Hence technology design should avoid capturing a detailed fingerprint trace whenever sensible.

To this end, the scanner captures traces by means of so-called coarse scans (Hildebrandt *et al.* 2012). Coarse scanning limits the pixel resolution of the captured image. Accordingly, one can only roughly see whether there is a fingerprint trace at a certain position of the luggage scanned ("region-of-interest"). However, the image's resolution is so low that one cannot distinguish one fingerprint trace from another; the image is blurred.

This approach of a coarse scan is not only important to speed up the scanning process and render it feasible to scan bags routinely but also promotes the criteria of:

- Avoiding personal data because data are anonymized, people cannot be singled out, treated differently, subject to specific error rates or comparison with incompatible databases, and additional knowledge from databases (wanted lists or AFIS) or audio/video material (CCTV recordings or work schedules) cannot be used;
- Avoiding a high scatter because detailed scanning is not applied to the entirety of captured data relating to all flights but only to a single bag which is scanned in detail after a bag was qualified as manipulated;
- The principle of transparency on systemic level because one can inform a third party after coarse scans and before detailed scans, that is, avoids identifiability and processing if the third party does not cooperate; and
- The principle of data minimisation because the technology is designed in a way that is not oriented towards processing personal data but only anonymized data; individuals do not have to fear data collection due to which they can be exposed to police follow-up measures.

4.2 Comparison within capture device (based on (Pocs 2011b))

The future crime prevention system compares the data captured on the spot of system deployment (about the large number of nonsuspects) with the wanted list. If it is a central database system, the system combines the movements of all data subjects in an information system of a single police department. Hence technology design should avoid unnecessary concentration of informational power about the movements of nonsuspects.

To this end, one can propose not to carry out the biometric comparison in a central database system but already within the capture device. For the comparison within the capture device, the police copy biometric data for the wanted list as index data from the central system into the capture devices. In order to be technically feasible, one needs to reduce the amount of data of a biometric dataset. For this, one can develop a data format using cryptoalgorithms of Biometric Template Protection.

This approach of decentralized comparison promotes the criteria of:

- Avoiding a high scatter because instead of the high number of persons that would be subject to the entirety of capture devices installed in the country, data capture is limited to the number of persons that are subject to a single capture device;
- The principle of data minimisation because the capture device does not necessarily copy the data into the central system;
- The principle of use limitation because it satisfies the requirement of (vertical) separation of informational powers;
- The principle of data security because it avoids the need for investment of time, money and expertise that would be needed to protect the captured data from all capture devices;
- Avoiding the use of uniform personal identifiers for comprehensive registration because not the location data from all capture devices but only the information about a certain place can be associated to the data subjects.

4.3 Distinction between data subjects (based on (Pocs 2011a))

In recent years the police obtained powers to collect data without justifying it by relying on a specific danger or suspicion. This broadens the group of persons (witnesses, contact persons, informants, victims, etc.). Further the police have the power to use another Member State's police information system ("Prüm") or the EU's police information system (SIS II). Hence varying traditions in terminology could lead to inadvertent broadening of groups of persons. For these reasons technology design should ensure distinction between the various groups of persons. The biometric system should only notify hits on the conditions for the inclusion into the wanted list specified by the legal provision.

To this end, one can propose to design the system in a way one can distinguish between the data subjects. The data fields used in the police databases enable the police to define the reasons of the registration of a wanted person. However, for the time being, the reasons the police use are not specific enough. They contain unspecific terms such as "international criminal." They include residual terms such as "other causes." There are also reasons such as "police observation" that do not distinguish between criminals, witnesses and contact persons. Therefore one has to define data fields so that one can distinguish between data subjects in line with the legal provision (suspect/nonsuspect, objects of legal protection with a high priority, etc.).

Further, for EU data exchange, one has to link causes and purposes used in police work with the equivalent terms of the own Member State's database. One can do this by using equivalent data fields and keys in a "table of equivalence." Finally, one has to consider that the police choose wanted lists after having begun to deploy the biometric system. Hence one should be able to evaluate the data processing afterwards and ascertain the actual size of the wanted list. To this end one should create an automatic counter of data subjects which counts the number of individuals that are subject to the wanted list. Otherwise the data needed may not be available anymore for evaluating the system deployment afterwards.

This approach of distinction between data subjects promotes the criteria of:

- Precision of legal provision because hits are only notified in the cases permitted by the law justifying the deployment of the biometric system;
- Avoiding a lack of cause or suspicion because the data subject has given cause for notification of hits; and
- Avoiding a high scatter because the group of persons subject to hits is limited.

4.4 Defining and testing of error rates

Biometric (one-to-many) identification systems are subject to specific error rates. Individuals could therefore be subject to false "hits." Technology design should hence limit the number of false hits and safeguard that the police comply with this limit during the system deployment.

To this end, one can propose several measures. As to the limit of false hits, one can choose between comparison algorithms. There are algorithms that are better at reducing the number of false non-matches and those that are better at reducing the number of false matches. In principle the latter algorithms should be preferred. Further, one has to establish the total working time of police officers to limit the number of false hits in a way that every hit is actually re-examined manually. The factors influencing

the error rates must not be alterable (physical position of capture device, comparison algorithms and thresholds of (dis-)similarity of faces, fingerprints, etc.).

Moreover one should consider several design requirements. The user interface should render the outcome of the comparison decision transparent. For example the system could display the relevant biometric features and the degree of similarity by means of "traffic lights." The captured data should be deleted without the need for human interaction. The police should train the operators of the biometric system regularly.

Moreover one has to safeguard compliance with the upper limit of false hits during the system deployment. To this end one should define the system during its testing and compare them with the subsequent deployment in real life. These aspects include: the physical position of capture device, comparison algorithms, thresholds of similarity, "population size" (number of data subjects), and the entire variability of data quality in the wanted lists. In addition one has to be able to evaluate the data processing afterwards and ascertain the actual number of false hits. To this end one should create an automatic counter of data subjects which counts the number of individuals that are subject to false hits (see above, 4.4).

This approach of defining and testing error rates promotes the criteria of:

- Avoiding coming under pressure to offer an explanation;
- Avoiding stigmatization;
- The principle of data accuracy;
- Avoiding automated individual decisions;
- The assumption of innocence;
- Equality; as well as
- The right to free movement and freedom to travel.

4.5 "Three-Step-Model" (based on (Desoi et al. 2011))

Biometric systems for crime prevention capture personal data without having established whether the captured data will be relevant for the police. This is only done during the data processing, e.g., if the security officer observes deviant behaviour. Even then, identification is not necessary in every case. Thus technology design should reduce identifiability of data subjects according to the level of danger and suspicion.

To this end, some propose a "Three-Step-Model" for biometric surveillance systems (Roßnagel *et al.* 2011) (Desoi *et al.* 2011). For fingerprint trace collection this means a variation of the scenarios mentioned above (section 2): During luggage handling at the airport, the police scan all fingerprint traces on bags. First, they scan the traces by means of so-called coarse scans (Hildebrandt *et al.* 2012). Due to their limited pixel resolution, one cannot use these data for identification.

Second, if there are more traces on the bags after the luggage handling process, one can suspect manipulation of the bags in the security zone of the airport. Then the scanner captures these new fingerprint traces by means of detailed scans. However, these data are not accessible yet. Third, if there is reason to believe that there is a specific danger or suspicion, the officer is authorized to access the data by receiving a decryption key or similar. However, even at this stage, one does not carry out identification yet, only if further investigation requires so.

This approach of reducing identifiability promotes:

- Reducing risks for the individuals according to the stages of danger and suspicion;
- Avoiding the high scatter of the data processing;

- The principles of transparency and control;
- The principle of data minimisation; as well as
- The principle of use limitation.

4.6 Exclusive storage of auxiliary data by data protection authority (based on (Pocs 2012a))

If the police desire to retain biometric data that enable them to identify suspects in case of an incident, one needs to store data about a large number of innocent citizens. Varying the scenarios mentioned in section 2, the police could scan all faces from CCTV cameras at the airport and store them for the duration of the flight. The police will not need most of the data but individuals have to be afraid of being exposed to police follow-up measures. Hence, technology design should remove identifiability and only re-personalize the data in case of an incident.

To this end, one can apply basic technologies of Biometric Template Protection on an institutional level. That is, the captured data are separated into so-called "pseudo identities" and "auxiliary data" and only a trusted third party such as the data protection stores the auxiliary data. In order to ensure that no one circumvents this, one also has to take several measures. For example one should separate system rights so that the police department cannot unilaterally change the system programs. Further, one should secure the exchange of keys and signatures between the police and the data protection authority.

Biometric Template Protection technologies, which are needed for the design approach of this subsection, do not work in all scenarios (just as the scenarios mentioned in section 2). This is because they only work after the system extracts features from biometric data which is necessary for automatic comparison. In that case one can take a similar but less strong approach of double encryption (Pocs 2012b).

This approach of institutional pseudonymization promotes the criteria of:

- Avoiding a high scatter;
- The principle of transparency by data separation on institutional level;
- The principle of data minimisation;
- The principle of use limitation by institutional separation of informational powers; as well as
- The principle of data security because not all datasets but only one dataset can be attacked at a time; and
- Avoiding using uniform personal identifiers for comprehensive registration because from the captured facial data random pseudoidentifiers are created and hence diversified so that the biometric data cannot be used as "access keys" to connect several databases; and
- Avoiding the obtaining of sensitive data because the system diversifies the captured biometric data and hence one cannot regenerate the original raw or template data from which one could obtain sensitive data about ethnic origin, health etc.

5 Conclusion

This paper derives technology design proposals from German and European legal requirements. Its aim is to avoid that individuals need to fear being exposed to

unnecessary police measures and “identity theft.” Thereby it contributes to the governance of science and technology using the example of future biometric systems for crime prevention (Table 1).

Society can only handle innovations in emerging technologies if governments are paying attention to both: the benefits of using technology, in this case, the protection from crime and dangers, on the one hand, as well as protection from consequences of abuse of informational power and carelessness when using that technology, on the other. If we take the opportunities privacy-enhancing design offers, it is possible to achieve both benefits for society.

Table 1. Overview of proposals for technology design derived from the law using the example of future biometric systems for crime prevention.

	"Coarse scans"	Comparison in capture device	Distinction between data subjects	Defining and testing errors	"Three-Step-Model"	Exclusive auxiliary data	…
Precision of legal provision			X				
Danger and suspicion					X		
Lack of cause			X				
High scatter	X	X	X		X	X	
Transparency	X				X	X	
Data minimisation	X	X			X	X	
Use limitation		X			X	X	
Data security		X				X	
Pressure/stigmatization				X			
Uniform identifiers		X				X	
Sensitive data						X	
Data accuracy				X			
Automated individual dec.				X			
Assumption of innocence				X			
Equality				X			
Free movement				X			

Acknowledgements

The work in this paper has been funded in part by the German Federal Ministry of Education and Science (Bundesministerium für Bildung und Forschung, BMBF) through the Research Programme under Contract No. 13N10820 - "Digitale Fingerspuren" (Digi-Dak).

Biography

Matthias Pocs, LL.M. (ICT law) studied Business and Labour law at Universität Hamburg and European law at University of Abertay Dundee in Scotland. As a Master of Laws, he completed studies in Information and Communication law at Leibniz Universität Hannover with prof. Wolfgang Kilian and at Universitetet i Oslo with dr. Lee Bygrave. In Brussels, he worked as a „Stagiaire" with the European Data Protection Supervisor (EDPS) Peter Hustinx. Currently, he is a member of a legal research group at the Universität Kassel where he is examining the legal aspects of automated fingerprint trace collection in the cooperative project „Digi-Dak" ("Digitale Fingerspuren"). He was also a guest researcher at the University of New South Wales in Sydney with prof. Graham Greenleaf. See publications referred to in this paper in full-text at <http://www.matthiaspocs.de/>

References

(Bundeskriminalamt 2007) Bundeskriminalamt (Federal Criminal Police Office), 2007. *Final Report of the "Fotofahndung" study at Mainz Railway Station* [online]. Wiesbaden, Bundeskriminalamt. Available from: http://www.bka.de/kriminalwissenschaften/fotofahndung/pdf/fotofahndung_final_report.pdf [Accessed 21 September 2012].

(Bouchrika *et al.* 2011) Bouchrika, A., *et al.*, 2011. On Using Gait in Forensic Biometrics. *Journal of Forensic Sciences*, 56 (4), 882–889.

(Brownsword 2006) Brownsword, R., 2006. Neither East Nor West, Is Mid-West Best?. *SCRIPT-ed*, 3 (1), 15–33.

(Bundesverfassungsgericht 1974) [1974] 37 BVerfGE 271.

(Bundesverfassungsgericht 1983) [1983] 65 BVerfGE 1.

(Bundesverfassungsgericht 1986) [1986] 73 BVerfGE 339.

(Bundesverfassungsgericht 1993) [1993] 89 BVerfGE 155.

(Bundesverfassungsgericht 2001) [2001] 100 BVerfGE 313.

(Bundesverfassungsgericht 2004) [2004] 110 BVerfGE 33.

(Bundesverfassungsgericht 2005) [2005] 115 BVerfGE 320.

(Bundesverfassungsgericht 2008) [2008] 120 BVerfGE 378.

(Bundesverfassungsgericht 2009) [2009] 120 BVerfGE 274.

(Bundesverfassungsgericht 2010) [2010] 125 BVerfGE 260.

(Bygrave 1998) Bygrave, L., 1998. Data Protection Pursuant to the Right to Privacy in Human Rights Treaties. *International Journal of Law and Information Technology*, 6 (3), 247–284.

(Citron 2007) Citron, D., 2007. Technological Due Process. *Washington University Law Review*, 85 (1), 1249–1313.

(Clarke 2009) Clarke, R., 2009. Privacy Impact Assessment, *Computer Law and Security Review*, 25 (2), 123–135.
(CNIL 2007) Commission nationale de l'informatique et des libertés (CNIL), 2007. *Biometrics* [online]. Paris, CNIL. Available from: http://www.cnil.fr/english/topics/regulating-biometrics/ [Accessed 21 September 2012].
(Commission 2009) Recommendation of the European Commission on PIA framework for RFID applications, C(2009) 3200, final.
(Commission 2012a) Proposal for a Directive of the European Parliament and of the Council on data protection in the police sector, COM(2012)10, final.
(Commission 2012b) Proposal for a General Data Protection Regulation of the European Parliament and of the Council, COM (2012)11 final.
(Daugman *et al.* 2004) Daugman, M., Malhas, C., 2004. Iris recognition border-crossing system in the UAE. *International Airport Review*, 2004 (2), 49–53.
(Desoi *et al.* 2011) Desoi, M., Pocs, M., and Stach, B., 2011. Biometric Systems in Future Crime Prevention Scenarios – How to Reduce Identifiability of Personal Data. *In:* Brömme, A., Busch, C., International Conference of the Biometrics Special Interest Group (BIOSIG 2011), 8–11 September 2011 Darmstadt. Bonn: Springer, 259–266.
(European Data Protection Supervisor 2010) OJ No C280, 16.10.2010, p. 1.
(Friedewald *et al.* 2010) Friedewald, M., *et al.*, 2010. Privacy, data protection and emerging sciences and technologies: towards a common framework. *Innovation: The European Journal of Social Science Research*, 23 (1), 61–67.
(Gates 2010) Gates, K., 2010. The Tampa "Smart CCTV" Experiment. *Culture Unbound: Journal of Current Cultural Research*, 2 (1), 67–89.
(Hammer *et al.* 1993) Hammer, V., Pordesch, U., and Roßnagel, A., 1993. *Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet.* Heidelberg, New York: Springer.
(Harcourt 2007) Harcourt, B., 2007. *Against prediction - profiling, policing, and punishing in an actuarial age*. Chicago: University of Chicago Press.
(Hildebrandt *et al.* 2011) Hildebrandt, M., *et al.*, 2011. Privacy preserving challenges: New Design Aspects for Latent Fingerprint Detection Systems with contact-less Sensors for Future Preventive Applications in Airport Luggage Handling. *In:* Drzygalo, P., *et al.*, *BioID 2011*, 4–6 March 2011 Brandenburg adH. Berlin: Springer Lecture Notes on Computer Sciences (LNCS) Vol. 6583, 286–301.
(Hildebrandt *et al.* 2012) Hildebrandt, M., *et al.*, 2012. Fingerspuren in der Tatortforensik. *Zeitschrift für Datenrecht und Informationssicherheit (digma)*, 12 (2), 80–83.
(Hornung *et al.* 2010) Hornung, G., Desoi, M., and Pocs, M., 2010. Biometric Systems in future preventive Scenarios – Legal Issues and Challenges. *In:* Brömme, A., and Busch, C., *Conference of the Special Interest Group on Biometrics and Electronic Signatures (BIOSIG 2010)*, 4–7 September 2010 Darmstadt. Bonn: Springer LNI, 83–95.
(Karyotis 2007) Karyotis, G., 2007. European migration policy in the aftermath of September 11. *Innovation – The European Journal of Social Science Research*, 20 (1), 1–17.
(Nissenbaum 1997) Nissenbaum, H., 1997. Towards an Approach to Privacy in Public - The Challenges of Information Technology. *Ethics and Behavior*, 7 (3), 207–219.

(NRC 2008) National Research Council, 2008. *Protecting Individual Privacy in the Struggle Against Terrorists - A Framework for Program Assessment*. Washington: National Academies Press.

(Pfitzmann 2006) Pfitzmann, A., 2006. Biometrie - wie einsetzen und wie keinesfalls? *Informatik-Spektrum,* 29 (5), 353–356.

(Pocs 2011a) Pocs, M., Gestaltung von Fahndungsdateien - Verfassungsverträglichkeit biometrischer Fahndungssysteme. *Datenschutz und Datensicherheit*, 35 (3), 163–168.

(Pocs 2011b) Pocs, M., Abgleich im Erfassungsgerät. *In:* Schartner, P., Taeger, J., *D-A-CH Security 2011*, 12–16 September 2011 Oldenburg. Oldenburg: syssec, 346–360.

(Pocs 2012a) Pocs, M., 2012. Vier Augen, zwei Behörden und eine Technik für künftige Biometrie-basierte Kriminalitätsbekämpfung. *In:* von Lucke, J., *et al.*, *Staat und Verwaltung auf dem Weg zu einer offenen, smarten und vernetzten Verwaltungskultur – Gemeinsame Fachtagung Verwaltungsinformatik (FTVI) und Fachtagung Rechtsinformatik (FTRI) 2012,* 15-16 March 2012 Friedrichshafen. Bonn: Lecture Notes in Informatics (LNI), 97–112.

(Pocs 2012b) Pocs, M., Schott, M., and Hildebrandt, M., 2012. Legally compatible design of digital dactyloscopy in future surveillance scenarios. *In:* Schelkens, P., *et al., Optics, Photonics, and Digital Technologies for Multimedia Applications II (SPIE Photonics 2012),* 2–6 July 2012 Brussels. Brussels: SPIE Vol. 8436, 84360Z (article number).

(Pocs 2012c) Pocs, M., 2012. Will the EU Commission be able to standardise legal technology design with a legal method? *Computer Law and Security Review,* 28 (6) (forthcoming).

(Roßnagel *et al.* 2011) Roßnagel, A., Desoi, M., Hornung, G., 2011. Ein Drei-Stufen-Modell als Vorschlag zur grundrechtsschonenden Gestaltung. *Datenschutz und Datensicherheit*, 35 (7), 694–701.

(SAPIENT 2011) FP7 research project SAPIENT, 2012. *Surveillance, Privacy and Ethics*. Karlsruhe, Fraunhofer-Institut für System- und Innovationsforschung. Available from: http://www.sapientproject.eu [Accessed 21 September 2012].

(Streinz 2011) Streinz, M., 2011. Die Rechtsprechung des EuGH zum Datenschutz. *Datenschutz und Datensicherheit*, 35 (9), 602–604.

(TeleTrust 2006) TeleTrust-Arbeitsgruppe Biometrie, 2006. *Kriterienkatalog zur Vergleichbarkeit biometrischer Verfahren (V3.0)* [online]. Berlin, TeleTrust. Available from: http://www.teletrust.de/uploads/media/KritKat-3_final_01.pdf [Accessed 1 October 2012].

(Thomas 1998) Thomas, R., 1998. As UK crime outstrips the US, a hidden eye is watching: Police switch on a camera that recognizes your face. *The Observer,* 11 October, p. 5.

(Working Party 2003) Opinion of the European Union's Article 29 Working Party on Data Protection of 1.8.2003 on Biometrics, WP80, 12168/02/EN.

(Working Party 2009) Opinion of the European Union's Article 29 Working Party on Data Protection of 1.12.2009 on the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, WP168, 02356/09/EN.

(Working Party 2010) Opinion of the European Union's Article 29 Working Party on Data Protection of 13.7.2010 on Accountability, WP173, 00062/10/EN.

(Working Party 2011a) Opinion of the European Union's Article 29 Working Party on Data Protection of 11.2.2011 on the revised Industry Proposal for a Privacy and

Data Protection Impact Assessment Framework for RFID Applications, WP180, 00327/11/EN.

(Working Party 2011b) Opinion of the European Union's Article 29 Working Party on Data Protection of 8.12.2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising, WP188, 02005/11/EN.