Biometric Systems in Future Crime Prevention Scenarios – How to Reduce Identifiability of Personal Data

Monika Desoi, Matthias Pocs, LL.M., Benjamin Stach

Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Forschungszentrum für Informationstechnikgestaltung (ITeG)
- Project Group Constitutionally Compatible Technology Design (provet) Member at the Interdisciplinary Research Center for Information System Design (ITeG) -
Universität Kassel, Wilhelmshöher Allee 64-66, 34109 Kassel
{ m.desoi, matthias.pocs, benjamin.stach }@uni-kassel.de

Abstract:
Biometric technology for crime prevention is emerging. The design of a biometric system is decisive for the protection of fundamental rights. This paper analyses the necessary reduction of identifiability of biometric data. By outlining the German legal framework, the paper assesses a technical design proposal for future biometric systems. In this context, a Three-Step-Model is suggested.[1]

1 Introduction

A passenger jumps out of a taxi and runs through the departure hall to the counter of the airline she is going to fly with. Meanwhile, she is observed by a video surveillance camera: The observation system's program alerts the airport security firm because of her rush. After having seen the video footage, the security officer classifies her correctly as no risk for security. Without being concerned by this the passenger checks in her luggage. Then her luggage is scanned for fingerprints, once just after the check-in and once before being loaded into the airplane. Checked with the database, the system says there are more fingerprints on the luggage at the second scan. The security personnel scans those fingerprints again and double-checks them manually. It turns out that all of the fingerprints belong to the passenger herself, so no further steps are taken.

This is a possible future scenario in which biometric data play a significant role. Police authorities have already deployed biometric systems in practice, e.g. face recognition [BK07] or iris scans at airports [DM04]. Respective research projects are funded, like 3D facial recognition [BN08], fingerprint scanning from luggage [Hi11] or behavioural pattern analysis by video surveillance. At the same time, existing biometric databases

[1] Acknowledgement: 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 Programmes under Contract No. 13N10820 – "Digitale Fingerspuren" (Digi-Dak), http://omen.cs.uni-magdeburg.de/digi-dak/, and Contract No. 13N10814 – "Verteilte, vernetzte Kamerasysteme zur in situ-Erkennung Personen-induzierter Gefahrensituationen (CamInSens)".

that contain data about crime scene traces as well as fingerprints and photographs from criminal records, are interconnected [PC05] and extended [ED07].

Due to these developments, it is possible that in the future laws will be enacted that for example allow the deployment of biometric systems at international airports for finding potential terrorists. Such a precautionary data capture, that is, before a danger is caused or a crime is committed, poses new challenges to the law [WP09] [He10] [Ho10] [Hi11], particularly because biometric characteristics are captured without the data subject having given cause for the capture and a large number of persons are subject to it. This paper focuses on the lawful deployment of biometric systems for future crime prevention scenarios. While this might not be realised in the short term, apparently, the fundamental rights involved will have to be addressed in the future. Therefore, this paper assesses whether or not the fundamental rights to privacy and data protection require the identifiability of biometric data to be reduced and how a biometric system has to be designed accordingly.

2 Opportunities and threats

New surveillance technologies provide the opportunity to prevent human failure due to long term operations (e.g. "monitor-blindness") in handling such systems. The gap between the occurrence of a threat, it's recognition on the screen and the intervention of police-forces can be shortened. On the one hand, this helps to avoid the risks of successful crimes. On the other hand, damage can be minimized and the chances of intelligence are improved.

Aside the great chances there are also risks. Primarily, there is a huge risk of violating the individual's right to informational self-determination. Due to the technologies a so called "total surveillance" is possible. The data obtained by new technologies can be matched with other reference data. Due to the growing amount of information and the development of analysis technologies, every information becomes richer in content. Biometric face recognition for examples allows automated identification of individuals based only on pictures taken by normal cameras in real time. Movement and personality profiles can be composed out of communication data, camera surveillance material – that is obtained at nearly every important traffic interchange and a huge number of other reference data sets. Even objects contain the information who handled them, e. g. when sophisticated analysis technology is able to read the fingerprints on them.

Technology design is a great opportunity to challenge those risks. The old copyright saying "the answer to the machine is in the machine" [Cl96] may not be the only way to abolish those risks, but is a huge part of that way.

3 Legal Framework

For the purpose of this paper, German law is considered. Firstly the concerned constitutional rights and secondly the sub-constitutional rights will be described.

3.1 General personality right (arts. 2 I i.c.w. 1 I GG)

The value and dignity of the person based on free self-determination as a member of a free society is a focal point of the order established by the Basic Law (GG, *Grundgesetz*). The general personality right as laid down in arts. 2 I i.c.w. 1 I GG serves to protect these values – apart from other more specific guarantees of freedom – and gains in importance if one bears in mind modern developments with attendant dangers to human personality [BV83] [Si84]. The general personality right is based on two fundamental constitutional rights: the right to inviolable 'dignity' in art. 1 I 1 GG and the right to 'self-development' enacted in art. 2 I GG. It contains amongst others the right to informational self-determination.

3.2 Right to informational self-determination

This right is understood as the authority of the individual to decide themself, on the basis of the idea of self-determination, when and within what limits information about their private life should be communicated to others [BV83]. The German Constitutional Court explicitly acknowledges that it is a prerequisite of free development of the personality under modern conditions of data processing; the individual needs protection against unlimited collection, storage and transmission of data relating to that individual [BV83].

However, the individual does not possess a right in a sense of an absolute mastery of their rights though. Rather they are a personality dependant on communication developing within the social community [Si84]. Information, even if personality based, is a reflection of social reality and cannot be associated exclusively with the individual concerned [BV83]. The tension between the individual and society has been decided by the Basic Law in favour of the individual being community related and community bound [BV83] [Si84].

Due to the principle of proportionality, deployment of a biometric system has to pursue a legitimate and lawful purpose, while no other means shall be available, which are as efficient as surveillance, but less intrusive. In particular, the danger for the right to informational self-determination must be adequate to the purpose pursued. Hence, the balancing here has one result: The bigger the danger for the involved rights, the more they interfere with the right to informational self-determination. In contrary this means, that the controller shall not deploy any intrusive methods, as long as there is no concrete danger.

Due to the limitation, that the deployment of a biometric system must pursue a legitimate purpose, all obtained data are bound to be processed only in compliance with this purpose [Al05]. Further, the principles of “data avoidance” and “data frugality” according to § 3a of the German Federal Data Protection Act (*BDSG*) provide that data processing systems be designed in a way that if possible (depending on the purpose and appropriateness) data are collected that cannot identify persons, their processing is little and their storage period is short [Ro11]. Removing identifiability may be pursued by means of separation of informational powers [BV83] according to which personal data as well as their processing must be split up so that control of data processing is limited according to the purpose of that processing.

To reduce the identifiability of personal data obtained by the biometric system, the system has to be designed in a way that all data are pseudonymized and protected against unlawful access. Following the principle that personal data should only be obtained and processed if necessary to pursue the legitimate purpose, those data should be impersonal (e.g. aggregated or non-person related) as long as possible. When the pursued purpose is fulfilled, those data shall be deleted or anonymized.

3.3 Are biometric data personally identifiable information?

The data protection principles apply if personal data are processed. Even for anonymous or pseudonymous data, precautionary rules are necessary to safeguard that those data stay anonymous or pseudonymous [Ro01]. It has been concluded that in biometric identification systems, biometric data are in general personal data [WP03] [Ho04]. Some even consider the biometric characteristic, the bodily material as such personal data [By10].

The definition of personal data needs to be interpreted in the light of the EU Data Protection Directive 95/46/EC (*DPD*) according to its art. 2 (a) i.c.w. Rec. 26 *DPD*. This definition has further been construed by the Art. 29 Working Party [WP07]. Pursuant to art. 30 *DPD*, this body is responsible for contributing to the uniform application of national implementations of the *DPD*. Biometric data are data about biological predisposition such as fingerprints and behaviour such as gait. Both categories are "any information"; indeed, they are a special data category because they are content information about a certain person as well as an element for connecting information and that person [WP07]. Biometric data derive from a "natural person" and are "relating to" [WP07] that person because they describe a person's health, ethnicity, etc., are used to treat suspects different from non-suspects as well as their use affects the interests due to error rates, insufficient distinction between data subjects [Po11], etc.

For assessing whether or not the person is "identifiable", one has to consider all the means likely reasonably to be used either by the controller or a third person. Criteria for this test may be the "lifetime" [WP07] of the biometric system, extent of the investment in the deployment of the biometric system, gravity of the possible interference, and existence of additional knowledge of the controller or third persons. The additional knowledge does not have to be a person's particulars; image and sound data are sufficient [WP04]. Reference databases such as wanted lists and criminal records may be used for the biometric comparison. Therefore, one may conclude that also systems for automated capture of biometric characteristics and comparison with wanted lists or deviant behaviour that aim at tracking down criminals, process personally identifiable information. Consistently, biometric systems have to be designed in a way that reduces identifiability of biometric data.

4 Design Proposal: Three-Step-System

To fulfil the legal requirements a Three-Step-Model has been developed as a technical and organisational design proposal [ ]. The proposed model is a way to meet the constitutional and legal requirements of data protection law. Those are especially the principle of proportionality and the principle, that all data should only be obtained and processed for specific and lawful purpose. The Three-Step-Model is a legally optimized routine for the operation of biometric surveillance systems. The main aim of the model is to reduce the intensity of the impact on fundamental rights, particularly the right to informational self-determination of a person monitored without any reason. Moreover, a scheme is given to the controller of the system for support in complex situations and difficult decisions to minimize any legal uncertainty.

The right to informational self-determination might be infringed by the acquisition, storage, or processing of personal data [Al03]. Processing involves the analysis of the data as well as their use for visual means (e.g. by displaying the monitored person on a visual display unit).

Therefore, the intensity of the impact can be reduced either by not storing the obtained raw data or by reducing the identifiability of a person as far as possible. As biometric data are important evidence in criminal proceedings – on which operating companies would most likely not relinquish – the Three-Step-Model makes use of the latter one. According to the Three-Step-Model, intelligent biometric surveillance units should avoid the identifiability of persons by the supervision personnel as much as possible. Hence, the basic setting provides the biometric data only in composed form (pseudonymised), e.g. pixelated on a visual display unit. The identifiability may only be restored stepwise according to reasonable grounds for suspicion; this depends on the extent of suspicion and the significance of the endangered legal asset as well as the degree of that endangerment. The identifiability of the observed person may only be restored to the degree that is essential for the investigation (of a crime).

The Three-Step-Model can be adapted to every automated surveillance system which supervises broad areas without any reason (such as airports or dangerous spots in rural areas) for suspicious behaviour and possible suspects by biometric means. On the first step the surveillance system monitors every person without any reason in the designated area. The aggregated biometric data are provided only in composed (pseudonymised) form to the supervision personnel. The identifiability of the monitored persons is not necessary for the outcome of the first step. If a person may be considered suspicious, they will be monitored selectively and if applicable classified (e.g. passenger of a flight). Only if this closer look confirms the suspicion, the ciphering will be lifted and the identifiability will be restored entirely.

4.1 Step 1: Observing Surveillance (depending on scenario, preferably broad collection of biometric data)

The first step is the basic setting. The scene will be under observing surveillance and the biometric data is broadly collected by special software.

As the system monitors without any reason, the personal data is pseudonymised. A visual display unit, for instance, could show the persons pixelated by point clouds or stylised as stick figures. The pseudonymisation is the default setting and can only be abrogated in particular cases.

The transition to the next step occurs automatically, if an accordant situation is detected by the software, or manually by the supervising personnel.

4.2 Step 2: Selective Monitoring

In the second step persons who give probable cause for suspicion because of their biometric data (e.g. because of their behaviour) are being monitored selectively. This might happen, for instance, by flagging the person concerned so that linked camera systems are able to track their behaviour or their routes. The purpose of this is to identify any current personal or collective danger.

As in step 1, the impact on the right to informational self-determination has to be reduced as much as possible. This is also ensured by pseudonymising the personal data. Moreover, the pseudonymisation itself is reduced to the necessary need to identify the legally relevant facts of a case. The biometric data that could identify a specific person (e.g. special proportions or tattoos) should be garbled as much as possible.

The transition to the third step occurs automatically only as an exception where a non-ambiguous situation occurs. As a matter of principle this step is taken manually by instructed supervision personnel.

4.3 Step 3: Identification (reconfiguration for preservation of evidence)

The third step conduces to the preservation of evidence. Therefore, the biometric data of the monitored person is displayed in an identifiable way to the supervision personnel. Hence, identification for the purpose of evidence is subsequently possible. A matching with (search) data bases is not yet allowed. When a person is identified within this third step, it can only be left to chance, for example where the identified person is linked with additional knowledge of the supervision personnel.

5 Conclusion

Concerning the surveillance system which use biometric data without any reason the Three-Step-Model is a necessary technical precaution to protect fundamental rights.

The complex process of balancing individual rights to informational self-determination on the one hand and danger to individual or public rights on the other hand can be structured and simplified by using the Three-Step-Model. Providing three precisely defined steps, describing a certain level of danger, the controller is utilizing different means, which are adequate to the level of danger. For controllers with no legal schooling, it is often difficult to decide in every situation, which kind of method is appropriate. The intensity of the intervention to informational self-determination, the legitimate purpose and further factors like the location of the systems are part of this balancing. For a lawful system deployment it is crucial to keep the intrusion to informational self-determination as little as possible. When a certain step of danger is reached, the controller progresses to a more sophisticated and more intrusive method.

The scenario at the beginning shows the feasibility of the Three-Step-System. Without it, personally identifiable information of the passenger would have been collected from the beginning. By implementing it, the identifiability of personal data is generally reduced.

Bibliography

[Al03] Albrecht, A.: Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, Nomos, Baden-Baden 2003.

[Al05] Albers, M.: Informationelle Selbstbestimmung, Nomos, Baden-Baden 2005.

[BK07] Bundeskriminalamt (BKA): final report „Fotofahndung“, http://www.bka.de/kriminalwissenschaften/fotofahndung/pdf/fotofahndung_final_report.pdf.

[BN08] Busch, C.; Nouak, A.: 3-D Face Recognition for Unattended Access Control, Datenschutz und Datensicherheit (DuD) 2008, 393.

[BV83] Bundesverfassungsgericht: BVerfGE 65, 1.

[By10] Bygrave, L.A.: The Body as Data? Biobank Regulation via the ‘Back Door’ of Data Protection Law, Law, Innovation & Technology 2010, 1.

[Cl96] Clark, C.: The Answer to the Machine is in the Machine, in: Hugenholtz, P. B. (ed.): The Future of Copyright in the Digital Environment, The Hague 1996.

[DM04] Daugman, J.; Malhas, I.: Iris Recognition border-crossing System in the UAE, International Airport Review 2004 (2), 49.

[ED07] Commission Drafts on Eurodac, 9/2009 & 10/2010; EU Council Conclusions 11004/07, 12.6.2007; EC Reg 2725/2000/EC, OJ EU 15.12.2000 L 316.

[Hi11] Hildebrandt, M.; Dittmann, J.; Pocs, M.; Ulrich, M.; Merkel, R.; Fries, T.: Privacy preserving challenges: New Design Aspects for Latent Fingerprint Detec-

tion Systems with contact-less Sensors for Preventive Applications in Airport Luggage Handling, in: Vielhauer, C. et al. (Eds): BioID 2011, LNCS 6583, 286, Springer-Verlag Berlin, 2011.

[Ho04] Hornung, G.: Der Personenbezug biometrischer Daten, Datenschutz und Datensicherheit (DuD) 2004, 429.

[Ho10] Hornung, G.; Desoi, M.; Pocs, M.: Biometric systems in future preventive Scenarios – Legal Issues and Challenges, in: Brömme, A.; Busch, C.: Conference Proceedings BIOSIG 2010, 83.

[HD11] Hornung, G.; Desoi, M.: "Smart Cameras" und automatische Verhaltensanalyse. Verfassungs- und datenschutzrechtliche Probleme der nächsten Generation der Videoüberwachung, Kommunikation & Recht 2011, 153.

[PC05] Prüm Convention, EU Council Doc. 10900/05; EU Council Decisions 2008/615/JHA and 2008/616/JHA, OJ EU L 210, pp. 1 and 12; 2010/482/EU, OJ EU L 238, p. 1.

[Po11] Pocs, M.: Gestaltung von Fahndungsdateien – Verfassungsverträglichkeit biometrischer Systeme, Datenschutz und Datensicherheit (DuD) 2011, 163.

[Ro01] Roßnagel, A.; Pfitzmann, A.; Garstka, H.: Modernisierung des Datenschutzrechts, Study for German Ministry of the Interior, Berlin 2001, pp. 107f.

[Ro11] Roßnagel, A.: Das Gebot der Datenvermeidung und –sparsamkeit als Ansatz wirksamen technikbarsierten Persönlichkeitsrechtsschutzes?, in: Eifert, M.; Hoffmann-Riem, W.: Innovation, Recht und öffentliche Kommunikation, Berlin 2011, 41.

[Si84] Simitis, S.: Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung, Neue Juristische Wochenschrift (NJW) 1984, 398.

[WP03] Article 29 Data Protection Working Party: Working document on biometrics (WP 80), Brussels 2003.

[WP07] Article 29 Data Protection Working Party: Opinion on the Concept of Personal Data (WP 136), Brussels 2007.

[WP09] Article 29 Data Protection Working Party: The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data (WP 168), Brussels 2009.