Proposal of a privacy-enhancing fingerprint capture for a decentralized police database system from a legal perspective using the example of Germany and the EU

Matthias Pocs[1], Mario Hildebrandt[2], Stefan Kiltz[2], Jana Dittmann[2]

[1] Stelar Security Technology Law Research UG (haftungsbeschränkt) c/o Fuchs, Fanny-Lewald-Ring 110, 21035 Hamburg
mp@stelar.de

[2]Research Group on Multimedia and Security, Otto-von-Guericke University, Universitaetsplatz 2, 39106 Magdeburg, Germany
{hildebrandt, kiltz, dittmann}@iti.cs.uni-magdeburg.de

Abstract: Innovations in biometric and forensic technology promise new use cases for the fight against crime and threats to public security. For example, the police will be able to use a new scanner to capture fingerprint traces from luggage at the airport to detect dangerous manipulations and identify known criminals. Despite these potentially great benefits, such systems also entail risks for society. One aspect of such systems is the biometric and forensic database used to compare fingerprints captured with a wanted list. This paper explores a possible decentralized database system as a solution to risks entailed by central systems. It uses the German and EU law as an example to justify technology design decisions on the basis of the legal requirements.

1 Introduction

The contact-less non-destructive acquisition and digital analysis of fingerprint traces, also known as digital dactyloscopy, creates new use cases. In this paper, a preventive use case at the airport serves as an example. Such use cases entail risks for individuals' privacy and society at large. We analyse the database aspect of such systems and a decentralized architecture as one possible solution to enhance privacy.

This paper is motivated by the privacy, policy and legal issues in biometric, forensic and security data. Only if the design of surveillance applications are strictly privacy-compliant the police will want to give orders to develop fingerprint systems for new use cases. Therefore this paper contributes to the improvement of privacy and data protection as well as the development of new database supported systems. This in turn extends the current police tool box because it means that additional data will be available for crime prevention.

This paper builds on a publication that explores the general legal requirement to use a decentralized database system [Poc11]. However that publication does not include the technical point of view. The transdisciplinary approach chosen in this paper ensures that both sides - lawyers and engineers - take each others' feedback into account. This is necessary for fairer legal regulation of privacy-enhancing technology design. Since this paper only looks at the database aspect, in Sections 3 and 4 other design aspects have to be integrated to assess the overall privacy impact. A second property of our approach is to distinguish general technical requirements (Section 4) from specific technical implementation (Section 5). This way technology is only required to follow design decisions as far as legally necessary, in this case the general technical approach (Section 4) is the legal requirement. The specific technical implementation (Section 5) shows examples of how to specify that general approach and are not binding. Nevertheless they are important because they enable technology producers to assess conformity with the legal requirement (for this approach see in detail [Poc12]).

The structure of the paper reflects the transdisciplinary approach we chose as lawyers and technologists. Section 2 outlines the technical use cases and their legal risks to derive to a design approach as a possible solution. In Section 3 this paper describes the state of the art from a technical and legal point of view. Whereas Section 4 gives the reader an idea of the general design approach, Section 5 specifies the technical implementation. Both sections build on legal arguments to justify design decisions. In the conclusion we sum up the technology design and its legal evaluation.

2 New use cases, risks and possible solution

In this paper we look at a use case that involves a fingerprint system used during luggage-handling at the airport [HDP+11]. It scans traces of fingerprints that are left on luggage. The police searches these traces on already known fingerprints from a database (of contact persons, criminals, or similar). In any case the captured data are strictly secured and deleted after the comparison. If there is a hit, the data are revealed for further investigation. This use case aims at gaining hints to detect terrorist and other criminal networks with histories of serious offences by means of identification of persons.

The use case offers opportunities of detecting dangerous persons suspected of serious crime. However, it also creates risks for the personality of individuals and society at large. In particular there are risks if one chooses to send all captured data to a central database system for comparison with a wanted list. In contrast to the IT security goals (confidentiality, integrity, authenticity, non-repudiation and availability), the main driver for this paper is the legal concept of privacy, which takes into account the following risks [MPD+13].

Sensitive data and identifiers. The capture of fingerprints and biological characteristics is already very risky for privacy. This is due to the fact that biological characteristics reveal unnecessary information about illnesses and ethnic origin (sensitive data). Additionally,

they are universal and life-long identifiers that can be misused to create a personality profile from databases and location data.

False hits. Furthermore there is a risk caused by the statistic errors involved in comparison of biological characteristics. In addition there is the risk of erroneous operation of the system by police officers. As soon as fingerprints are compared by the police with fingerprints of wanted persons, people could be confused with terrorists or other criminals.

Function creep. Moreover there is the risk of "function creep." The legislator can introduce the fingerprint system using the fight against serious crimes as a justification and subsequently allow its use for less important purposes. For example, ministers and senior police officers, who want to punish minor offences or take measures against non-criminals, can urge parliaments to allow this. The German AFIS contains fingerprints of three million people [Bun12] among which there are many that are not a terrorist or a similar criminal. The secretive capture of fingerprints even increases the risk of function creep.

Technology compliance. There is the risk that the police procure and use a noncompliant fingerprint system. There are no EU wide standards for security technologies [EDT09]. Therefore there is an increased need for checking whether the system design reducing the privacy impact is on paper only or a reality.

"Identity theft." In addition, there is the risk of "identity theft." A minister or senior police officer could "attack" the fingerprint system in order to achieve a successful result of a search, that is, use the system in a way that is not authorized by the law. Even such illegitimate aims, the law needs to consider ([PoS76], 208). They could use databases to track political activists, discriminate against ethnic groups and less important purposes without legal authorization.

Follow-up measures. Besides, there is the risk of being exposed to a follow-up police measure. This is due to fact that fingerprint traces are captured and made available to the police which were not before. Citizens can be exposed to police measures due to the risks of function creep, identity theft and false hits. They may feel like being watched and abstain from deviant behavior, which harms society at large. The fact that a large number of innocent citizens are involved due to the large "scatter" of the data processing increases all of the risks mentioned above.

A possible solution to these risks (in connection with other privacy-enhancing measures) is the approach of a decentralized database architecture where the captured data are compared within a local subsystem attached to the capture device. Only in cases of a confirmed hit they are re-examined in a central system. For such a decentralized database system, one needs to reduce the amount of data that is necessary for the performance on small IT systems.

3 State of the art and legal requirements

From a technical point of view we need to assess the state of the art of biometric and forensic systems. In biometric systems we can use one-to-many identification or one-to-one verification to identify fingerprints or similar [Viel06]. The biometric community has also explored techniques to protect biometric templates (standardized in ISO/IEC 24745:2011). However, the technical possibilities for forensic use cases are limited because until recently the community primarily considered use cases with controlled situations. That is, the system captures fingerprints or similar directly from the individual or a representation of such a direct collection. This way the quality is sufficient to properly carry out identifications and verifications.

However in forensic use cases the original fingerprint is not available. Instead the system captures latent fingerprints / fingerprint traces. In this case the fingerprint quality is usually low because the fingerprints might be only partial, smeared, distorted or similar. Thus, other matching strategies need to be applied.

One potential technique to protect the privacy of biometric data as well as taking into account the variations in the data is the application of biometric hash functions [SSM05, TFM+07]. Unlike cryptographic hash functions such techniques are designed to generate similar hashes for similar data representation, similar to the piecewise hashing outlined in [BaB11], and thus, allowing for a matching in the hashed. In [SSM05] such an authentication scheme is evaluated for the example of facial images. This particular approach combines a user-dependant one-way transformation and secure hashing algorithms. Another approach is introduced by Tulyakov et al. [TFM+07] for the example of fingerprints. This technique uses symmetric hash functions to compute biometric hashes for sets of minutia points (see e.g. [HRL11]), which results in a set of hashes for each fingerprint. The symmetric hash function has the advantage that all elements are equally weighted. Hence, the hash is not depending on the order of elements. Furthermore, each minutia is represented by a complex number with additional factors to address potential differences in rotation and translation of the fingerprint. During the matching process the hash sets are compared with each other while retaining the matches with the highest confidences. This technique might also help to address the issue of partial and smeared latent fingerprints. Thus, it is considered in our concept in Section 4. However, the potential for reverse-engineering biometric traits, such as described by Kümmel et al. [KuV10], needs to be analyzed.

As mentioned in Section 1 we cannot regard the approach of a decentralized database in isolation to improve privacy protection. We also have to consider other privacy-enhancing design approaches. New basic technologies such as the so-called “coarse scan” and “aging” promise to minimize the number of fingerprints captured in order to spare innocent people police investigations [DVU+12] [MPD+13]. Another design approach, the “Two-Offices Principle,” employs a double encryption technique [PSH12]. This ensures that the police can only use fingerprints captured when they indicate a threat to public security because they may belong to a known dangerous person. A third design aspect is the proper error management. Besides an automated matching, which is prone to errors especially for low quality fingerprint data, there are manual approaches.

In the case of the forensic analysis of fingerprints we employ a four staged investigation technique [HRL11]. This ACE-V methodology consists of the analysis, comparison, evaluation and verification steps. In order to achieve high standard of matching decisions two forensic experts follow this methodology independently of each other.

In addition to the technical assessment we have to explore the specific legal privacy requirements for new surveillance applications using digital fingerprint systems.

System suitability and effectiveness. The first privacy requirement is that the system needs to be suitable to achieve the stated purpose, which is, identifying criminals. One has to consider the system performance and economic reasonability. This means that the hits and fingerprints have to be available to the police when they need them. In order to be effective, the system needs to reduce false hits and help the police do so [MPD+13].

Use limitation. Another privacy requirement is that the system needs to limit the data use to the stated purpose of the fight against crime. The system should prevent the police from exploiting health and ethnic data from fingerprints [Art03] (see Article 8 of the European Data Protection Directive [Dir95]). The system should also prevent the police from exploiting fingerprints as uniform identifiers for personality profiles. This is prohibited by the *Bundesverfassungsgericht* (German Federal Constitutional Court).

To prevent unnecessary exploitation, the system should also erase non-hits instantly and securely. This requirement follows the *Bundesverfassungsgericht,* which rules out a privacy impact for non-hits that are not communicated to a police officer and instantly erased. In order to prevent data disclosure for secondary use, one has to ensure that only the police department in charge can use the data. This "separation of informational powers" is required by the *Bundesverfassungsgericht*.

Data security. The system needs to be secured by technological means against identity theft by considering user rights management, secure communication and state of the art cryptography. This is also a new requirement of Article 27 of the Directive Proposal for Police Data Protection [Com12a].

Transparency. Another privacy requirement is transparency. The system needs to enable courts and supervisory authorities to understand when and which police department used certain data in the past. It means that the fingerprint scanning system needs to be able to log when and where fingerprints are scanned and who collects them.

Accountability. System users need to demonstrate that the technology design required by the law corresponds with its actual realization. They have to take measures for compliance with the privacy requirements and implement mechanisms for auditors to verify the effectiveness of these measures. This is a new requirement of Article 22 of the Data Protection Regulation Proposal [Com12b]. This means that system users need to prepare source codes and documentation of programs, tools and hardware.

Data minimization and "data frugality." The system should avoid the collection of unneeded personal data or pseudo-/anonymize them. This requirement of data minimization, more precisely, "data frugality" is defined in § 3a of the *Bundesdatenschutzgesetz* (German Federal Data Protection Act). This means that the

system should use anonymous data instead of personal data and reduce the number of data categories and data retention period.

Distinction between individuals. Another privacy requirement is to distinguish criminals from innocent citizens. One has to distinguish between people having committed minor offences and serious crimes, between suspects and non-suspects as well as suspicion on the basis of mere assumptions and those based on facts. The latter two distinctions are new requirements of Articles 5 and 6 of the Directive Proposal for Police Data Protection [Com12a]. The system should help the police focus on serious criminals and spare any other person, already known to the police, follow-up measures.

Avoidance of large scatter. One has to avoid that a large number of persons is exposed to the system. This avoidance of a large "scatter" of data processing is required by the *Bundesverfassungsgericht*. This means that the system should reduce the scatter of data capture and use [HDP+11].

4 General design approach and improvement of privacy protection

For the use case mentioned in the introduction, we propose the general design approach of a decentralized database system with the setup shown in Figure 1.

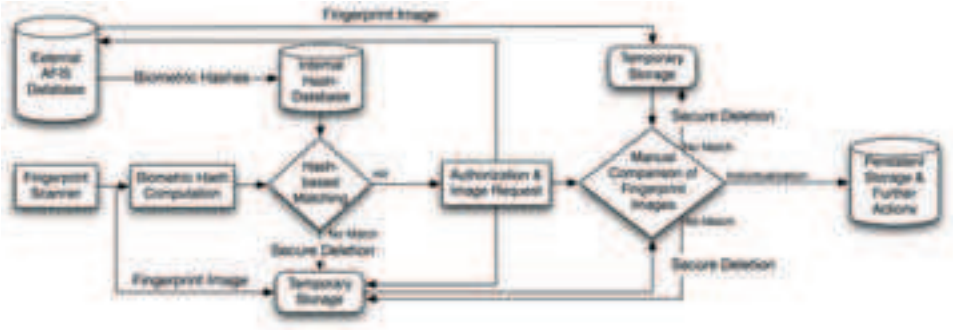

Figure 1: General design approach of a decentralized forensic fingerprint matching system

The system scans latent fingerprints at the airport using a contact-less scanner and computes the corresponding biometric hash (in line with ISO/IEC 24745:2011 (V60.60, 17.6.2011)). In parallel, the fingerprint image is stored within a temporary storage, which meets the demands regarding the security aspects of integrity, authenticity and confidentiality. Furthermore, a small internal database with biometric hashes is created from a main central database system such as AFIS (see [HRL11]). The local database stores only selected biometric hashes from the external AFIS database that relate to people having committed serious crimes or caused threats to someone's life or the state.

This small database is searched by comparing stored biometric hashes with the computed hash from the captured fingerprint. This leads to an automatic pre-selection of data sets by means of *multiple verifications of biometric data* as opposed to a full identification against a large database. In contrast to AFIS, which has the goal of a low false non-

match rate (FNMR), a low false match rate (FMR) should be achieved by this system to avoid mis-identifications. If no matching biometric is found within the local database, the fingerprint image in the temporary storage is securely deleted (see e.g. [Gut96]).

If the system finds a "hit" in the small database, this results in granting the forensic expert the permission to retrieve the image of the fingerprint from the data captured at the airport and to receive the reference image from the central database (e.g. AFIS). The expert does not have access to the entire database but only one set of fingerprint images that has been identified using the fully automated pre-selection of the data. The necessary fingerprint images for the matching samples are automatically requested from the central database. Hence, the fingerprint image from the external database needs to be stored in a temporary storage. Thus, at this stage, only an individual set of fingerprint images that indicate a threat to public security are stored.

The general approach of a decentralized database can be integrated into the overall set of privacy-enhancing design approaches. Concerning the basic technologies "coarse scan" and "aging" there is no conflict with the decentralized approach. The detailed scan necessary for the decentralized matching is independent of the "coarse scan" and "aging", which aims to preselect the fingerprints to be captured. The "Two-Offices Principle" can also coexist with the decentralized database system. These privacy protections even strengthen each other because the fingerprint images can be secured in a way that the system only releases them if a trusted third party has checked that there is a reason to do so. Also the decentralized database adds to the proper error management. After the captured fingerprint images are released to the forensic expert, a manual comparison is performed by a forensic expert. If the expert has the opinion that the fingerprints are not matching (exclusion), both fingerprint images are securely deleted from the temporary storage. If the fingerprints are matching (individualization), the fingerprints are transferred to a persistent storage and further actions are performed, e.g., arresting of the suspect and transfer of the data to central law enforcement agencies.

The implementation of the general design approach of a decentralized database improves privacy in several ways. This is because it promotes the legal requirements mentioned in Section 3.

System suitability and effectiveness. With the decentralized database the system does not lose its suitability to achieve the purpose of identifying criminals. The use of biometric hashes enables even small IT systems to perform well. The decentralized database even improves the data availability for local police departments who are in charge. However, reducing the calculation time through the use of biometric hashes can also lead to an increase in false hits caused by collisions of the hashes. However the decentralized approach also means that there is an additional round of manual re-examination by forensic experts at the local database system. Hence the false hit rate is decreased for the entire system.

Use limitation. The decentralized database ensures that the police only use the system for the purpose of the fight against crime. Exploiting health and ethnic data as well as uniform identifiers can be better prevented in isolated local IT systems that only serve a specific purpose than in a large-scale central system with multiple purposes and multiple

users. Also the instant and secure data erasure is only possible in such systems. Moreover using decentralized databases the system can ensure that only the police department that is in charge can use the data (separation of informational powers).

Data security. The decentralized database improves data security. In comparison to a multi-purpose system like a national AFIS, a local system with a more specific purpose can better ensure correct user rights management. With the decentralized database the local system does not communicate the large number of data about innocent citizens to a central system. This saves costs for the securing of communication channels and the stored data. However the choice of multiple isolated local systems increase the costs for keeping the encryption algorithms up-to-date.

Another advantage for data security is the use of the improved possibility to delete unneeded data. Both the captured fingerprint images and the reference fingerprint images are stored in a local temporary storage. Only if the forensic experts confirm the matching of fingerprints in a manual examination procedure, they are transferred into a persistent storage. In doing so, only a few fingerprints are stored within the database and the challenge of a secure deletion within the local database is avoided.

Transparency. The use of a decentralized database improves transparency because it only works if the data exchange between police departments is properly logged. Otherwise the link between the references of the local and the central system would be lost and this would disable the police to take measures against a suspect.

Accountability. The current use cases of central database systems like AFIS have a lesser privacy impact than the new use cases at the airport. This is why there are stricter requirements for the preparation of program source code and system documentation. If one chooses to use the central system, there is the risk that the police only refer to existing documentation prepared under less strict requirements. In case of a decentralized database system the police cannot do so. They are more likely take the accountability requirements seriously.

Data minimization and "data frugality." The use of biometric hashes can anonymize the fingerprints captured. It can also reduce data categories by using an index data system for the decentralized database. Only after associating the fingerprints with the original database the police can reveal more information about the wanted person.

Distinction between individuals. With the decentralized approach one can better ensure distinction of criminals from innocent citizens. Assuming that the number of wanted persons is much smaller for the new use case at the scenario any large database is likely to include other people too. In a local system for a specific purpose the performance is limited and one can limit the storage capabilities. This way one can ensure that the police only use a small database focusing on serious criminals.

Avoidance of high scatter. The main privacy improvement is that the decentralized database enables the system to preselect relevant fingerprints, which reduces the "scatter" of the data processing to a minimum.

5 Specific technical implementation and legal evaluation

In order to implement the general approach of a decentralized database system we have to address a number of measures. These measures include the implementation of the decentralized database approach. We explore several aspects of it: the type of comparison and generation of biometric hashes, connection between the central and decentralized system, user rights management, design of the local devices and central system as well as encryption of data and communication. In addition we look at the integration of the decentralized approach into the entire system including a backup strategy. Whenever a certain design decision is legally necessary, we refer to the legal requirements described in the previous section.

In contrast to other fingerprint identification systems such as AFIS, the "identification" is performed using multiple verifications (one-to-one comparison) and no ranked list is displayed. This is necessary, because ranked lists need to be verified by experts manually, which would cause a lot of work at the decentralized system. Furthermore, a list with 15 candidates contains at least 14 mis-identified samples. In a one-to-many comparison all samples with a limited similarity are selected, which are used to create the ranked list (see e.g. [JFN+12]). Usually, such approaches include special index structures to avoid the more time consuming one-to-one comparison. Such an approach would lead to a high scatter, which should be avoided within a preventive system.

The system we propose performs the comparison using biometric hashes to reduce the amount of data which is necessary for the performance on small IT systems. The local database contains one table, "reference_data", with biometric hashes as primary keys and corresponding authorization codes to request fingerprint images from the external database. However, we can also identify several limitations of using techniques of biometric hash, in particular, the false match rates. Whereas the goal of AFIS is a low false non-match rate (accidently missing the matching trace), the goal of this system needs to be a low false match rate for *avoidance of high scatter*. For *system suitability and effectiveness* we need to strike a balance. The use of biometric hashes has to provide the performance needed for small IT systems but also must ensure a low number of false hits. Reducing the information in hashes also serves other legal requirements. It improves *use limitation* since it removes sensitive data. For *data security* it is less likely to be able to reconstruct the original fingerprint image from a hash with reduced information. For *data minimization and "data frugality"* they are more likely to be considered anonymous data.

In particular the system architecture needs to rule out the possibility to reconstruct the original fingerprint image as reported e.g. by Cappelli et al. [CML+07] for the reconstruction from biometric templates. In the recent years, many researchers analyzed the reversibility of several fingerprinting and robust hashing algorithms. The hashes used in our system architecture should be robust to a so-called reversibility attack and spoofing to avoid attacks as described e.g. in [KuV10] for a biometric hash for handwriting. In general such reconstruction approaches lead to samples that are likely to be matched using automated systems. However, the risk of a reversibility attack is not

high because for human experts several differences in the fingerprint trace and reference are visible.

There also needs to be a link between the biometric hash and the image representation of the fingerprint. Since the local database only contains biometric hashes and authorization codes that associate data sets with those in the central database, the system is restricted to the minimum amount of information. Such an index data architecture meets the requirement of *system suitability and effectiveness*. If the local reference database reveals all information about wanted persons, criminals can use that information to jeopardize the purpose of the fingerprint system. In case of index data the local database does not reveal the fingerprint image or biographic information, only the biometric hash and an index number. The index data approach also meets the *transparency* requirement. If forensic experts follow up on a hit using the full fingerprint image, they need to request the reference fingerprint image from the central system. This way another police department obtains knowledge about the fact that the police department at the airport found a hit. For *data minimization and "data frugality"* the index data means that the system reduces data categories to the category of hashes and index data.

The user rights management for the database has to ensure that forensic experts can only access the fingerprint images in case of a hit. Several databases need to be secured from unauthorized use. The access to the "reference_data" database has to be restricted in such a manner that only the biometric hashes are accessible using a special database view for the user. In addition the local fingerprint scanner captures fingerprint images. For each image, a biometric hash is computed. A second table, "capture_data", needs to store the biometric hashes generated from the local fingerprint scanner, as well as meta data and a reference to the fingerprint image within the temporary storage. This database also needs to be secured from unauthorized access.

In a local system one can better control the storage capabilities. The size of the temporary storage can be limited in a way that the "reference_data" does not exceed a certain population size. This way only a small selection of wanted persons can be detected and a routine identification of a large number of citizens is avoided. For *distinction between individuals,* this is beneficial because only the most important criminals should be addressed [Poc10]. Otherwise a large reference database could be used, which, does not sufficiently distinguish people causing serious threats from others such as victims, witnesses and contact persons.

For the temporary storage devices appropriate deletion mechanisms need to be used. Such techniques are dependant on the utilized storage concept. In general the stored data should be overwritten with new data. Thus, storage media with wear levelling mechanisms, such as solid state disks should be avoided because of the uncertainty with which such devices manage deleted data [BeB10]. Another option is the encryption of each stored fingerprint image using an individual key. If the key is deleted from the storage, the image data is rendered inaccessible. The key itself must be overwritten but this is much faster compared to the deletion of the entire fingerprint image due to the limited amount of data of the key.

In order to create the table “reference_data” the system needs to download the selected biometric hashes in regular time periods from the central system. Whereas there needs to be a connection between the central and the local system, the data should only flow in one direction. One must not be able to upload the data captured at the airport from the decentralized database to the central system (read only) or pull those data from the central system. Otherwise the legal advantage of the general decentralized design approach is lost. The restriction to read-only access can be easily achieved using rights management. The connected user of the local system should gain access to a limited view which allows for accessing one particular image that corresponds to the authorization code from the local database “reference_data”. In addition this should be ensured by restricting the list of references in the central system too. Just like the limitation to a selection of most important criminals in the local system’s table “reference_data” mentioned above, a list of potential hashes should be provided within the central database to limit the amount of accessible data to a list of most important targets.

We have to look at the need to encrypt the database and communication channels. Each captured fingerprint image in the temporary storage can be encrypted using an individual key. In this case the key needs to be stored within the database as well. The temporary storage can be a separate database or a special file system. Either way a sophisticated access restriction and secure deletion mechanisms are necessary. For *use limitation* such additional encryption can improve secure data erasure. For *data security* it can prevent “identity theft.” Although there is little information included in the biometric hash, the need for securing the database is still urgent because the system also stores the fingerprint images. This is different for the securing of the communication channels between the central and the local system. In relation to *data security* the local system does not communicate the large number of data about innocent citizens to a central system. The need to secure the communication channels is less urgent. Regarding the database encryption, for *data security* it is required to keep the encryption algorithms up-to-date. The communication channels within the local system, as well as the communication channel between the local system and the central database need to be encrypted with state-of-the-art algorithms, too. Furthermore, each communication partner should be authenticated to avoid any unauthorized access to the data. This also applies for the system that is used for the manual comparison since it needs to display both images. The displayed data must be deleted securely from any storage devices. The disclosure of data has to be limited by organizational means (e.g., avoiding the displays to be photographed) and by technical means (e.g., disabling USB ports).

The measures for the decentralized database can be integrated into the other privacy-enhancing design approaches, most notably, the proper error management in case of a match. The automated matching of the biometric hashes is performed using a stored procedure, which executes the comparison during the insert query. If a matching pair of biometric hashes is found in the database, the authorization code of the matching fingerprint is used to request the corresponding fingerprint image from the external database. This image is stored in another temporary storage device. Furthermore, in a third table, “investigation_data”, the matching pair of biometric hashes is stored, accompanied by the references to the fingerprint images within the temporary storages.

Additionally, an examiner is alerted that a matching pair of fingerprints is found, which requires a manual investigation. The examiner can access the relevant data from the table "investigaton_data" containing the references to the fingerprint images, as well as necessary encryption keys. In addition the system has to generate secure log files (with regard to the security aspects of integrity and authenticity) that enable supervisory authorities to check the police measures. If the examiner concludes that the images are matching, the data is stored within a separate database to allow for further actions. If no match is found, the fingerprint images in both temporary storages are securely deleted and the status of the investigation in the table "investigation_data" is deleted. If the database contains any encryption keys, a secure deletion of such keys is also necessary.

With this step the local investigation is completed. If the fingerprints are matched, there is a reasonable suspicion to continue a forensic investigation. This involves law enforcement agencies and thus, the transfer of the collected data. To ensure the validity of the data as potential evidence, it is necessary to fulfill all requirements regarding the security aspects of integrity and authenticity. Furthermore, the local expert should have a proper training similar to forensic experts at the forensic laboratories, to avoid mis-identifications. This also includes the documentation of the analysis according to forensic standards.

Another factor is the application of backup and recovery strategies. Since the reference hashes can be obtained from the central database, no backup is required. Furthermore, biometric hashes from acquired fingerprints should be stored temporarily, thus, those data do not require a backup, either. If the biometric hash based identification resulted in a hit, there is a vital interest of preserving the data until the investigation is finished. Thus, the table "investigation_data" as well as the temporary storages need to employ backup strategies. Since the match is not confirmed at this stage of the investigation, measures such as redundant storage, e.g., redundant arrays of independent disk (RAID) devices, and protection against external influence factors, e.g., the application of uninterruptible power supplies and shock absorbers, should be used. Further techniques should be used after the individualization of the fingerprint. Here, the data needs to be protected until it is handed over to the law enforcement agency. This could include the storage on WORM (write once, read many) media. Such media can be also used for the transfer to the law enforcement agencies. The suggested backup strategies and their implementation however have to meet the legal requirements, e.g., the sensitive data and identifiers (see Section 2) must be securely deleted (see Section 4). This applies either if the suggested hit is a false match or the earmarked and justified time of data retention is reached.

The entire design needs to be evaluated towards its feasibility. It is necessary that potential collisions of the biometric hash do not lead to mis-identifications. Furthermore, such collisions should only occur rarely because otherwise an increased amount of manual analysis time would be necessary.

6 Conclusions and future work

In this paper we explored how technology design decisions can improve the legal privacy requirements in fingerprint systems for new surveillance use cases. For their database aspect we demonstrated that it is legally preferable to take a decentralized database approach. In addition, we discussed specific decisions of technical implementation using legal arguments. Technology producers can use the descriptions of this paper for the documentation of program source code, tools and hardware. This way the paper also helps the police and other users comply with the legal requirement of accountability.

We integrated the database requirements into the other elements of the system so that legislators can assess the overall privacy impact of future digital dactyloscopy. In addition, we distinguished the general approach of a decentralized database from the specific measures. This way legislators can draw a clear dividing line between legal obligations and legal incentives. If technology producers take the specific measures we developed, conformity is presumed, but they can also develop more innovative measures to fulfill the general requirement.

The local database system explored in this paper contributes to a future digital dactyloscopy that reduces the privacy impact for a large number of innocent citizens at the airport.

In future work the performance of biometric hashes for the verification and identification of biometric traits in forensics should be analyzed. Furthermore, potential weaknesses of such approaches towards the reconstruction of biometric data, as well as collisions of hashes should be investigated.

References

[Art03] Article 29 Working Party on Data Protection (European Board of Data Protection Authorities): Opinion on Biometrics (WP83), EU Publications Brussels, 2003, no. 3.7.

[BaB11] Baier, H.; Breitinger, F.: Security Aspects of Piecewise Hashing in Computer Forensics. In 6th International Conference on IT Security Incident Management and IT Forensics (IMF), Stuttgart, Germany, IEEE Computer Society, ISBN 978-1-4577-0146-7, DOI=10.1109/IMF.2011.16, 2011, pp. 21-36.

[BeB10] Bell, G.; Boddington, R.: Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery? In Journal of Digital Forensics, Security and Law, Vol 5. No. 3, 2010, pp. 1-20.

[Bun12] Bundeskriminalamt (German Federal Criminal Police Office): http://www.bka.de/nn_227308/DE/ThemenABisZ/Erkennungsdienst/Daktyloskopie/AFIS/afis__node.html?__nnn=true, Wiesbaden, 2012.

[Com12a] European Commission: Proposal for a Directive of the European Parliament and of the Council on data protection in the police sector (COM(2012)10 final), EU Publications Brussels, 2012.

[Com12b] European Commission: Proposal for a General Regulation of the European Parliament and of the Council on data protection (COM(2012)11 final), EU Publications Brussels, 2012.

[CML+07] Cappelli, R.; Maio, D.; Lumini, A.; Maltoni, D.: Fingerprint Image Reconstruction from Standard Templates. In IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 29, No. 9, 2007, pp. 1489-1503.

[Dir95] Directive 95/46/EC of the European Parliament and of the Council on data protection. Official Journal of the European Union L 281, 1995, p. 31.

[DVU+12] Dittmann, J.; Vielhauer, C.; Ulrich, M.; Pocs, M.: Fingerspuren in der Tatortforensik. In digma - Zeitschrift für Datenrecht und Informationssicherheit, 2012, p. 80-83.

[EDT09] ECORYS NL; DECISION Études et Conseil; TNO: Study for European Commission on the Competitiveness of the EU security industry, EU Publications Brussels, 2009.

[Gut96] Gutmann, P.: Secure Deletion of Data from Magnetic and Solid-State Memory. In Proc. 6th Usenix Security Symposium, San Jose, California, USA, USENIX Association, 1996, pp. 77-95.

[HDP+11] Hildebrandt, M.; Dittmann, J.; Pocs, M.; Ulrich, M.; Merkel, R.; Fries, T.: Privacy preserving challenges - New Design Aspects for Latent Fingerprint Detection Systems with contact-less Sensors for Future Preventive Applications in Airport Luggage Handling. In Proc. BioID 2011, Springer Lecture Notes on Computer Sciences (LNCS) Vol. 6583, Springer, 2011, p. 286.

[HRL11] Holder, E.H.; Robinson, L.O.; Laub, J.H.: The Fingerprint Sourcebook, U.S. DoJ, Office for Justice Programs, 2011, Chapter 6.

[KuV10] Kümmel, K.; Vielhauer, C.: Reverse-engineer methods on a biometric hash algorithm for dynamic handwriting. In Proc. 12th ACM workshop on Multimedia and security, 2010, pp. 67-72.

[MPD+13] Merkel, R.; Pocs, M.; Dittmann, J.; Vielhauer, C.: Proposal of Non-Invasive Fingerprint Age Determination to Improve Data Privacy Management in Police Work from a Legal Perspective using the Example of Germany. In (Garcia-Alfaro, N. et al. eds.) Proc. 7th International Workshop Data Privacy Management (DPM 2012), Pisa, Italy, 2012, Lecture Notes in Computer Science, Vol. 7122, 2013 (forthcoming).

[Poc10] Pocs, M.: Gestaltung von Fahndungsdateien - Verfassungsverträglichkeit biometrischer Systeme. In Datenschutz und Datensicherheit (DuD), 2010, p. 163-168.

[Poc11] Pocs, M.: Abgleich im Erfassungsgerät. In (Schartner, P.; Taeger, J. eds.): Proc. D-A-CH Security, Oldenburg, 2011, syssec, 2011; p. 358.

[Poc12] Pocs, M.: Will the European Commission be able to standardise legal technology design without a legal method? In Computer Law & Security Review, 2012 (forthcoming).

[PoS76] Podlech, A.; Steinmüller, W.: Informationsrecht und Informationspolitik, Oldenbourg Verlag, 1976, p. 211.

[PSH12] Pocs, M.; Schott, M.; Hildebrandt, M.: Legally compatible design of digital dactyloscopy in future surveillance scenarios. In (Schelkens, H. et al. eds.) Proc. Optics, Photonics and Digital Technologies for Multimedia Applications, SPIE Photonics 8436, Brussels, 2012, p. 84360Z.

[SSM05] Sutcu, Y.; Sencar, H.T.; Memon, N.: A Secure Biometric Authentication Scheme Based on Robust Hashing. In Proc. 7th ACM workshop on Multimedia and Security, 2005, pp. 111-116.

[TFM+07] Tulyakov, S.; Farooq, F.; Mansukhani, P.; Govindaraju, V.: Symmetric hash functions for secure fingerprint biometric systems. In Pattern Recognition Letters 28, 2007, pp. 2427-2436.

[Vie06] Vielhauer, C.: Biometric User Authentication for IT-Security - From Fundamentals to Handwriting. In Advances in Information Security, Springer Science+Business Media Inc., ISBN 0-387-26194-X, 2006.