Privacy preserving challenges: New Design Aspects for Latent Fingerprint Detection Systems with contact-less Sensors for Future Preventive Applications in Airport Luggage Handling

Mario Hildebrandt[1], Jana Dittmann[1], Matthias Pocs[2], Michael Ulrich[3], Ronny Merkel[1], Thomas Fries[4]

[1] Research Group on Multimedia and Security, Otto-von-Guericke University Magdeburg, Universitaetsplatz 2, 39106 Magdeburg, Germany
{hildebrandt, dittmann, merkel}@iti.cs.uni-magdeburg.de;
[2] Projektgruppe verfassungsverträgliche Technikgestaltung (provet), Universität Kassel, Wilhelmshöher Allee 64-66, 34109 Kassel, matthias.pocs@uni-kassel.de;
[3] State police headquarters Saxony-Anhalt, Luebecker Str. 53, Magdeburg, Germany, michael.ulrich@polizei.sachsen-anhalt.de;
[4] FRT, Fries Research & Technology GmbH, Friedrich-Ebert-Straße, 51429 Bergisch Gladbach, Germany, fries@frt-gmbh.com

Abstract. This paper provides first ideas and considerations for designing and developing future technologies relevant for challenging privacy-preserving preventive applications of contact-less sensors. We introduce four use-cases: preventive detailed acquisition of fingerprints, coarse scans for fingerprint localisation, separation of overlapping fingerprints and age determination for manipulation detection and automatic securing of evidence. To enable and support these four use-cases in future, we suggest developing four techniques: coarse scans, detailed scans, separation and age determination of fingerprints. We derive a new definition for the separation from a forensic approach: presence detection of overlapping fingerprints, estimation of the number of fingerprints, separation and sequence (order) detection. We discuss main challenges for technical solutions enabling the suggested privacy-preserving use-cases combined with a brief summary of preliminary results from our first experiments. We analyse the legal principles and requirements for European law and the design of the use-cases, which show tendencies for other countries.

Keywords: latent fingerprints, preventive application, contact-less fingerprint acquisition, legal requirements

1 Motivation

The detection of latent fingerprints with new contact-less sensors is a new challenge in forensics when investigating crime scenes (e.g. see [1]). Those sensors are recently investigated (not yet applied in the field) and allow new application areas by a faster

and more detailed and non-destructive acquisition. Before such sensors can be used practically several aspects need to be investigated. The overall research questions are for example related to the quality of fingerprint acquisition and detection on different surfaces. As future applications might include the usage in crime prevention scenarios, additional questions of privacy preserving technologies and application approaches arise. They include, but are not limited to, challenging research questions by having to consider data minimality need to be answered before the release of such applications. This becomes a necessity because fingerprint data is personal data and subject to privacy and data protection laws [2]. Stringent precautions need to be taken since traces of innocent people are scanned a priori. The scenarios include, but are not limited to, large crime scenes, dangerous environments or security checks of luggage and freight. The technology of high quality contact-less scans might enable scenarios, which include automatic verification or even identification of latent fingerprints. However, due to high error rates (reported in the range of 93.4% accuracy for the verification in [3]) an automatic identification of potential "endangerers" is not considered, yet. Thus, the traditional subjective assessment of the fingerprints by a dactyloscopic expert remains the recommended approach. Furthermore, an automatic verification or authentication gathers data about innocent people and increases risks of misuse. Hence, such scenarios are not regarded due to legal, ethical and societal reasons. However, today fingerprints are taken often anyway at border controls where potential "endangerers" could be identified with the help of their exemplary fingerprints and their photograph. Thus, our goal is to introduce first ideas and considerations for designing and developing future technologies relevant for challenging privacy-preserving preventive applications and their legal requirements for European law. These are used to show tendencies for European and other countries. We provide preliminary approaches and results by showing tendencies and potential future technical possibilities. However, our focus for experiments is limited in this paper.

Our idea is to divide the acquisition into *coarse scans* for the manipulation detection (if someone touched the luggage without permission) and *detailed scans* of fingerprint for further manual investigations (if there is any indication of a malicious activity) in an airport luggage-handling use-case. We suggest that *coarse scans* are used for the automatic localisation of fingerprints on a particular surface (Regions-of-Interest). The advantage of such a coarse scan is that no visible fingerprint patterns allowing for a verification of the fingerprint are present in the acquired data; thus they preserve privacy. We suggest *detailed scans* by capturing at a much higher resolution, depending on the particular surface and the quality of the latent fingerprint even level 3 features [5], such as pores on the ridge lines, can be detected. We show first tendencies towards those techniques, too. Furthermore, we suggest using the *Separation of overlapping fingerprints* to analyse multiple fingerprint patterns on the same position. Derived from a forensic approach, we define four phases of the separation: *detection of the presence of overlapping fingerprints*, *estimation of the number of involved fingerprints*, *separation of overlapping fingerprint patterns* and *sequence (order) detection*. The sequence detection is a first *age detection* and we propose to use further *absolute age detection* to estimate the point in time a particular fingerprint was left on the surface. First results provide promising data; however, the feasibility of the short term age detection has to be evaluated in large scale tests in future work. In the following, we introduce the basic technologies of our suggested *coarse scans* for

fingerprint position determination and verification, *detailed scans* to support forensic investigations, *separation of overlapping fingerprints* and *age detection* of latent fingerprints, as fundamentals for the four basic privacy-preserving use-cases *coarse detection*, *detailed detection*, *separation and age detection* and *securing of evidence*.
We analyse the legal requirements for privacy and data protection for each use-case. The European privacy and data protection principles are lawfulness, purpose limitation, necessity and proportionality, data minimality, data accuracy, data sensitivity, transparency (that is, participation and accountability), supervision by data protection authorities, data security, and privacy by design [2]. The results of a preventive collection of latent fingerprint data that enables an identification or verification have to be earmarked on storage. Access to the stored data should be highly restricted and an automated secure deletion must be performed if the data is no longer needed.
This paper is structured as follows: Section two provides an overview of currently available contact-less sensors actually considered in research for forensic investigations, which are capable of capturing latent fingerprints from surfaces. Section three summarises the legal principles. Section four introduces our ideas towards basic technologies as fundamentals for the four use-cases and shows first tendencies for the localisation of fingerprints using *coarse scans*, as well as for *detailed scans* of the detected fingerprints and first results of the *age detection*. In section five our ideas for the design of the potential fingerprint detection systems for the four new use-cases are introduced. The legal requirements for the use-cases are analysed in section six for the European legislation to show tendencies for other countries. Section seven summarises the content of this paper and provides an outlook to the future work.

2 State of the art of contact-less fingerprint acquisition devices

The contact-less acquisition of latent fingerprints without any treatment, which is used in crime scene investigation, is a challenging problem. From several known approaches, see e.g. [4, 8, 9, 10, 11], in this paper we currently use a FRT MicroProf200 equipped with a chromatic white light (CWL) sensor [11], which captures intensity and topography data of the surface. Different contact-less sensors are currently researched in more detail. The approach from [4] uses a digital camera with a polarisation filter to reduce the specular component of the reflected light of the fingerprint residue while still capturing the specular component of the surface reflection for the contrast enhancement. However, the exact positioning of the light source, the camera and the polarization filter angle is necessary to get a usable result. The CWL sensor uses a beam of white light and the effect of chromatic aberration of lenses. The wavelength with the focal length exactly matching the distance to the surface is reflected most; this enables an exact determination of the distance to the surface by the sensor. Additionally the amount of reflected light is recorded for each point. We use differential images of one area with and without a fingerprint to determine which information is visible to the sensor. Engel and Masgai use a FRT MicroProf with CWL sensor [7] for the acquisition of latent fingerprints in 2004. In 2008 the technique of optical coherence tomography is adopted by Dubey et al. [8] for the detection of latent fingerprints under a layer of dust. Other sensors include [9], where 2D fingerprints are lifted from curved surfaces and [10] where fingerprints on absorbing surfaces should be ascertainable.

For the evaluation of our first approaches in this paper, we use a MicroProf200 with CWL 600 sensor [11], since it is commercially easily available and provides topography data, which might be useful for the separation and age detection. Furthermore, this device is a multi-sensor device and can be tuned for higher scan speeds and different surfaces. It is used to show first tendencies for the utilisation of contact-less fingerprint scanners. In theory this technique allows for an automatic identification of fingerprints. However, even the verification of latent fingerprints with exemplary fingerprints has been reported in the range of 93.4% accuracy (see [3]). Hence, the current algorithms must be improved to enable a reliable identification of fingerprints. Additionally, an automatic identification without a particular suspicion is not necessary. Thus we introduce four new promising use-cases for the application of such sensors in section 5; they are designed to be privacy-preserving and compatible with ethical and legal requirements.

3 Legal principles

This section outlines the legal principles in relation to the fundamental rights of persons whose fingerprints are scanned. By deploying the fingerprint scanning system, fundamental rights of individuals may be interfered with [22]. If personal data is collected, the deployment interferes with the right to privacy and data protection [15]. This interference triggers protection under the European privacy and data protection principles (see section 1). According to the principle of privacy by design, the interference can be qualified on the basis of the application design. Thus, design proposals could establish the legality of the preventive application of the fingerprint scanner. In particular, the legal assessment in this paper focuses on the use-case 5.2 (detailed detection) for securing evidence for future criminal prosecution. The goal is to draft legally relevant elements of technology design.

The detailed scan (5.2 to 5.4; see section six for the coarse scan) aims at identifying persons no later than on criminal prosecution. With access to these data the police can identify persons subject to AFIS (automated fingerprint identification system) and other reference databases. However, also the data about persons that are not subject to AFIS are personal because they represent “factors specific to [the data subject’s] physical identity” according to Article 2(a) Data Protection Directive and the detailed scan allows to distinguish one from the other [16] [17]. In addition, these data are unique and lifelong valid so that relating data to an identifiable person is more likely. Besides, identifiability may also derive from extra information; for example, from the time of leaving a fingerprint and the working schedule one might relate the fingerprint to an employee [17]. The interference can be justified by purposes that serve public interests if the interests pursued with the use-cases are proportionate to the gravity of the interference. In section six the proportionality is analysed.

4 Our design approach

In our paper we focus on the acquisition of fingerprints with the FRT MicroProf 200 using a CWL sensor to show tendencies for preventive fingerprint acquisition systems. In the actual settings of our test, we consider a working distance of 6.5mm [11]. In particular first results for the coarse and detailed fingerprint detections as the fundamental requirement for such systems are shown. The overall technical solution is

future research work. In this section we discuss and introduce four basic technologies as fundamentals for the privacy-preserving use-cases in section 5.

Design of coarse scan for fingerprint detection and localisation (4.1). In our setting used, the CWL is a point sensor; the amount of points for measuring significantly affects the total acquisition time. Our idea of a first approach of coarse scans with this CWL is a trade-off between acquisition time and result quality. Our first results indicate that a point distance of 400µm (63.5dpi) is sufficient for the localisation of fingerprints. Using the CWL sensor fingerprint residue usually appears darker than the surface material (Fig. 1). Hint: this effect is not or not as obvious on absorbing surfaces with our actual CWL setup, but can be achieved with enhanced sensor settings, which are considered in our further research.

Fig. 1. Coarse scan of smooth black plasic surface with fingerprints

Fig. 2. Automatically identified fingerprint positions

Our idea generally is to determine the variance of the intensity within segments to a global mean of the complete surface. In the first step segments with variances exceeding a surface dependent threshold are marked as possible Regions-of-Interest (see the small grey squares in Fig. 2). In a second step, nearby regions are combined to bigger Regions-of-Interest. If a region exceeds the size of 5x5mm it is automatically marked as a possible latent fingerprint location (see white rectangles in Fig. 2). As evaluated in first tests, this approach currently works on non-absorbing smooth surfaces, such as various hardtop cases (e.g. plasic or polished metal); a section of 10x10cm can be currently acquired and analysed within 10 minutes. With enhanced sensor settings, appropriate algorithms for different surface materials need to be investigated. This is necessary for a reliable detection of fingerprint positions on every kind of luggage. Our experimental work shows here already very good indications.

Design of detailed scan for fingerprint verification and identification (4.2). Our idea of detailed scans is to support further investigations of the fingerprint patterns for verification, and in theory identification, of the particular fingerprint on all three feature levels (see [5]). They require a much higher acquisition resolution compared to coarse scans. Our exemplary first tests are performed at a distance of 10µm between two measured points (2540dpi), which enables, depending on the fingerprint pattern and the surface material, a detection of pores (level 3 features in [5]). The fingerprint ridgelines are visibly darker than the surface material; the pores on them are visible as brighter spots. From our first tests, the overall quality of the acquired data is dependent to the surface material. The first test set is limited to smooth, non-absorbing surface materials, which provide the best results with our current algorithm.

Definition and design of overlapping fingerprint detection (4.3). The separation of overlapping fingerprints is a challenge to our current research. It is mostly an enhancement for the detailed scan, since the coarse scan does not provide enough data for the separation. Regarding overlapping fingerprint detection from a forensic point of view, we divide it into four different objectives: detection of the presence of overlapping fingerprints, estimation of the number of involved fingerprints, separation of overlapping fingerprints, sequence (order) detection. The detection and separation of

overlapping fingerprints is necessary for the discrimination between multiple fingerprint patterns at the same position on the luggage, e.g. on the locks or handle. In respect to the state of the art, there is several works on separation of overlapping fingerprints such as [12] or [13]. Singh et al. [12] use independent component analysis to separate overlapping fingerprints. In [13] an approach to separate two overlapping fingerprints under ideal conditions is introduced, requiring a significantly different angle, to be able to determine the different orientation fields. However, the used fingerprints are developed, e.g. by carbon black powdering. Work in respect to sequence detection can be found in [14]; here it is observed that the first fingerprint pattern is interrupted by the overlaying one. However, different residues are applied to the fingers prior to imprinting the fingerprints to the surface to enable the separation and sequence detection. The sequence detection is a special form of the age detection, which determines the relative age between multiple fingerprints; it does not determine the absolute age of each fingerprint. To our knowledge, there is currently no work in respect to all four different objectives of overlapping latent fingerprints for contact-less acquisition, supporting different kinds of surfaces (e.g. rough, absorbing or textured) without pre-processing such as carbon black powdering.

Design of fingerprint age detection (4.4). The age detection is necessary to estimate a certain point in time, when a particular fingerprint was left on the surface (*absolute age*). This allows for the selection of only the relevant fingerprints, avoiding the storage of fingerprint data of uninvolved or innocent people. Prior work discovered a degeneration of features and ridge line width as aging effects and that closed pores might merge or become open pores [6]. They investigate aging effects of latent fingerprints over a time frame of two years for relative age detection. It is highly dependent on the original pattern, since, to our knowledge, without the information of the initial ridge line width and pore size and distribution the estimation of the fingerprint age with optical sensors is not possible, yet. The possibility of the age detection for very small time intervals with contact-less sensors should be evaluated in future work in more detail. Our first experiments with the CWL (3x3mm, 3-10µm) use a *differential age detection* approach to investigate the aging of the residue. Therefore, multiple scans of the same area of a fingerprint are performed in short intervals for a time span of ten hours using a test set of four fingerprints (one of which is exemplary shown in Fig. 3).

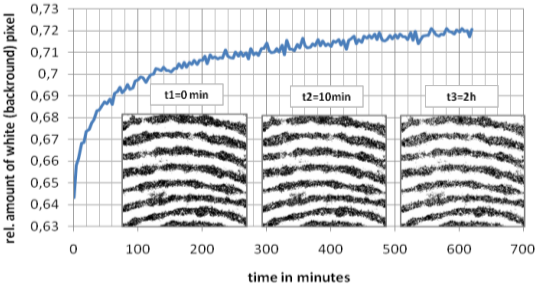

Fig. 3. The increase of the white (background) pixel of a binarised fingerprint image part (3x3mm, 300x300 pixel) in relation to the time passed. In the right corner the binarised fingerprint is shown at three points in time (t1=0 min; t2=10min; t3=2h)

To our knowledge, most curves of natural processes are either logarithmic, exponential, or, in some cases, linear. Our idea is to study the amount of changes within the captured image caused by water evaporating from the print involved when a fingerprint trace is left on a surface. A possible way of measuring this fact is counting the black/white pixels in a scanned and binarised fingerprint intensity image, representing the amount of residue which is present. The curve of such an aging-feature is logarithmic over time, as shown in Fig. 3 for an exemplary fingerprint part (3x3 mm, 10µm).

Overall perspective for the design approaches and their technical challenges. From the overall perspective, the localisation of fingerprints using a coarse scan is our first step for the fingerprint acquisition. The second step is the detailed scan of each identified position. If an overlapping fingerprint pattern is detected in the detailed scan, the number of patterns is determined and all fingerprints have to be separated. Subsequently, the order of overlapping fingerprints (*relative age*) and the *absolute age* for each fingerprint should be determined. We are currently able to successfully locate the fingerprint positions with our experimental CWL setting on smooth surfaces; the detailed acquisition of fingerprints is possible on such surfaces, too. Research questions are here how to improve the acquisition of fingerprint patterns from rough, textured and/or absorbing surfaces. First tests indicate that the approach can be modified to work on textured veneers or brushed metal. The evaluation of short term age detection using contact-less optical scanners in large scale tests to confirm our first results remains future work. The *absolute age* detection can reduce the number of fingerprints that are acquired in detail; thus, non relevant fingerprints are not captured, which supports the privacy preserving application. This also applies for *relative age* detection where only the overlaying pattern is necessary in most cases. Currently, *differential age detection* using multiple scans can be performed. Furthermore, other sensors like digital cameras should be evaluated for a localisation of fingerprints on bigger areas. All four aspects of the separation of overlapping fingerprints on various surfaces remains future work for contact-less scans of latent fingerprints.

5 Design of preventive applications to enhance airport luggage handling security systems

Based on our approaches introduced in section 4, the fingerprint acquisition can be integrated into the available luggage handling systems. Potential applications are derived and illustrated in the use-cases *coarse detection*, *detailed detection*, *separation and age detection*, as well as *securing of evidence* (all shown in Fig. 4). We show exemplary implementations for these use-cases in the following subsections.

Coarse scan system for fingerprint location verification (5.1; coarse detection). The idea of *coarse scans* supports the detection of the fingerprint positions. From the first experimental setup, our current algorithms only work on smooth, non-absorbing surfaces. A possible system for fingerprint location and position verification is shown in Fig. 4(a). Our objective is to use such a system for the detection of the manipulation of the luggage during the automatic luggage processing by detecting changes of the number and positions of fingerprints. After the check-in an initial coarse scan is performed. It determines the locations of all fingerprints and stores only a bounding box for each position (see Fig. 2). Afterwards, the usual automatic luggage handling

with the security scans takes place. Before the luggage is prepared for the manual loading to the airplane, a new coarse scan is performed.

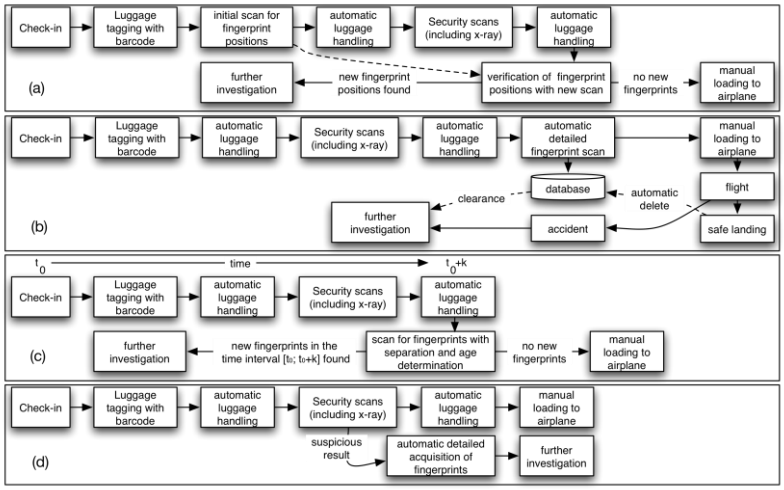

Fig. 4. Illustration of use-cases: (a) coarse detection, (b) detailed detection, (c) separation and age detection, (d) securing of evidence

If new fingerprint positions are found during the verification of positions, the particular piece of luggage is separated for further investigation. This might include a detailed scan of the additional fingerprint positions for the purpose of securing of evidence. However, no detailed fingerprints are acquired and stored a priori; only the new fingerprints are acquired, fulfilling the minimality principle (Section 1).

Scan system for detailed fingerprints (5.2; detailed detection). Our proposed *detailed scans* of fingerprints on luggage can be a useful preventive use-case. However, the access to the acquired data should be highly restricted and as soon as possible unneeded data must be securely deleted automatically. Our general idea for such a system (see Fig. 4(b)) is to perform a *detailed scan* of fingerprints prior to the manual luggage loading and to keep them until the airplane has landed safely. Then the acquired fingerprints are automatically securely deleted from the database. However, the secure deletion from databases remains future work. If an accident or serious incident happens during the flight, the acquired data for this particular flight is cleared for further investigations. The fingerprint data should only be used earmarked for this particular case.

Scan system with detection of fingerprint age and overlapping fingerprints (5.3; separation and age detection). Our idea is to use the *separation, sequence and age detection* of fingerprints to reduce the number of necessary scans of the luggage to one. This might be possible if the *absolute age* of the fingerprint can be determined and overlapping fingerprints can be separated. The Fig. 4(c) shows the modified system. Here our idea is to locate and acquire fingerprints prior to the manual loading of the luggage to the airplane. If new fingerprints that are applied in the time frame between the check-in time t_0 and the scan time t_0+k are found, a further investigation is performed. The separation and age determination of fingerprints most likely requires a detailed scan (although, a very small area of the fingerprint might be sufficient for

the age detection). In this case, the acquired data must be securely deleted instantly, if no trace of new fingerprints is found in the timeframe between t_0 and t_0+k. However, if new fingerprints are detected, those particular fingerprints newer than t_0 can be used earmarked for further investigation. This implements the stated goal of the minimality principle (section 1). However, to our knowledge, the determination of the *absolute age* is currently not feasible. Therefore, we suggest performing a *differential age determination*. From the curve shape (see Fig. 3 in section 4.4), we can derive, that there is the tendency of water evaporating from the print within the first hours, which gives us the possibility for our considered privacy preserving use-case. For this purpose a small portion of the fingerprint must be scanned two times t_0+k-t_Δ and t_0+k shortly before being loaded onto the aircraft with an exemplary time span, such as $t_\Delta=10min$ in between these two scans $((t_0+k-t_\Delta)-(t_0+k)=10min)$. The white pixels of both scans can then be counted and their difference calculated. Since the aging curve is logarithmic, a high difference-value accounts for an early stage in the run of the curve and therefore a young age ($age < k$) of the print. This can be considered suspicious, since nobody should have touched the luggage since the check-in. In such a case the suspicious fingerprint can then be investigated further with the help of a detailed scan.

Automatic securing of evidence (5.4; securing of evidence). In this case our idea is to connect the fingerprint acquisition system with the existing security scans. If one of the present security scan systems detects something suspicious, e.g. possible drug smuggling, the fingerprints on the particular piece of luggage are acquired in detail for the securing of evidence. Hence, this use-case, as shown in Fig. 4(d), differs from the prior use-cases; it relies on a precisely defined suspicion. This exemplary system separates the suspicious luggage directly after the security scan that initiated the investigation and acquires the fingerprints with a separate contact-less latent fingerprint acquisition device. The automatic securing of evidence is very useful, since the fingerprints are preserved prior to the further investigation. This is beneficial if the original fingerprint patterns are destroyed due to the investigation. However, the acquired data should be used earmarked and should be securely deleted if the initial suspicion could not be approved.

6 Analysis of legal issues for the defined use-cases

In this section, we show potential legal challenges for the use-cases. Particular attention is drawn to the use-case “detailed detection” (5.2), in order to establish and optimise legal compatibility. Regarding the coarse scan (5.1), no personal data is collected if single fingerprints cannot be distinguished from a sufficiently large number of other fingerprints [17]. This inability also excludes the assertion of other legal violations (e.g., discrimination). However, this exclusion presupposes that individual scans are not otherwise related to specific passengers. For example, video and audio material of surveillance cameras or working schedules must not reveal such a relationship. In the application scenario this is not the case. Therefore, coarse scans can even serve as privacy-enhancing technology if they limit detailed scans to manipulated or dangerous luggage.

The interference (see section 3) caused by the detailed scans (5.2 to 5.4) can be justified if the use-cases answer a “pressing social need” [18]. They answer such a need

because they enable the police to take purpose-specific measures and allow for a new reach of police observation (e.g., in Germany [19]). However, the principle of proportionality requires that the use-cases be proportionate to the gravity of the interference with the fundamental rights to privacy and data protection. Where manipulation or dangerous luggage content indicates a source of danger (5.1, 5.3 and 5.4), the interference is proportionate since the data subject has given a reason for the police to act and the luggage is examined immediately after capturing the fingerprints and the captured data is deleted securely without further use if the result is negative.

In the use-case "detailed detection" (5.2), proportionality of the interference has to be assessed in detail. To this end, the European privacy and data protection principles give guidance: a) the interference is grave because the data subject has not given a reason (e.g., suspicion) for the capture of his fingerprints (purpose limitation); b) due to the secretive nature of the fingerprint capture, citizens might feel like being watched and therefore not exercise their rights freely (transparency; in Germany, e.g. [20]); c) unique data with lifelong validity facilitate connecting different databases (purpose limitation); d) sensitive data may be extracted from fingerprints (sensitivity; hence, minimising sensitive data for comparison with AFIS and other reference databases should be object of future research). There is also the societal dimension of privacy and data protection: the number of citizens that are subject to interference without having given a reason for it, may be significantly large and therefore create the risk of abuse of political power (societal data protection [21]).

In contrast, secondary use of fingerprint data is avoided by technology design and organisational measures. The data is secured from access for purposes other than those specified (see below), the data accessed are the ones relating to the flight in question (data accuracy), and all data related to other flights are automatically deleted when the airplane has landed. It does not allow human interaction like CCTV cameras. If only the data related to a flight where an accident occurs are accessed, the interference is similar to that at conventional crime scenes. Overall the gravity of the interference depends on whether or not the number of citizens is significantly large.

On the other hand, the more important the goal pursued by the use-case is, the more grave interferences it can justify. This "preventive use-case" aims at facilitating investigations of an accident or other serious incidents by securing evidence beforehand. The goal has to be further specified (purpose limitation). For example, it could be required that the incidents put at risk the security of the state or individuals' lives, bodies or freedom, or constitute a crime specified due to its range of penalties and the extent of wrongdoing in the particular case is taken into account. Further, passengers of the flight in question may not be suspects. The importance of the pursued goal depends on whether or not there is suspicion (based on facts and criminalistic experience), and whether or not the suspicion is still valid (erasing data about others as soon as the offender has been found).

In order to justify the capture of fingerprint data for which the individuals have not given reason, the system design can be optimised. In the case of the Data Retention Directive 2006/24/EC, it is accepted to store data for future crimes because numerous companies control smaller databases, avoiding a centralised database (societal data protection), and the data controllers are not the executing police authorities which creates transparency of data access (transparency). Consequently, the legislator should also provide that the captured data is controlled by several police (or even non-police)

authorities. Regarding the large number of citizens at airports, such system architecture optimises compatibility with the fundamental rights to privacy and data protection (privacy by design).
The overall interference is grave for both citizens that are not subject to further use as well as those who are. Therefore, the legal, organisational and technical guarantees for both groups are subject to particularly strict requirements. These requirements can only be fulfilled if not only legal but also organisational and technical guarantees are laid down in a legally binding manner (data security; see, e.g. [23]). Finally, the deployment of the technology (5.2 to 5.4; except for the coarse scan) has to be provided for by law (lawfulness). Concerning the use-cases where the manipulation or the dangerous content of the luggage indicates a source of danger (5.3 and 5.4), specificity and safeguards of the legal basis do not have to meet high standards. Therefore, general provisions about police data collection and use suffice. Concerning the capturing of fingerprints without suspicion in order to obtain evidence for future prosecution (5.2), general police provisions on data processing do not suffice. Hence, a legal basis needs to be introduced that specifically lays down this use-case. Depending on the interference with the societal dimension of data protection, clarity of the purpose specification, technology design, and organisational safeguards, introduction of a legal basis may also be in line with the fundamental rights to privacy and data protection.

7 Summary and Future work

This paper provides a first exemplary design of preventive applications utilising contact-less fingerprint acquisition sensors for four exemplary use-cases. We show first tendencies for the localisation of fingerprints and their detailed acquisition as part of the basic technologies representing the fundamentals for the use-cases. The legal assessment suggests that there are design approaches that may be decisive to avoid that the highest courts in Europe veto the preventive application of the fingerprint scanner. Future work should concentrate on the improvement of the available sensors and algorithms to improve the quality of the results and to reduce the surface material dependency to fit the requirements of a preventive application and further specification of the application to prepare legal instruments. Furthermore, the basic technologies of separation of overlapping fingerprints including the relative age detection and the absolute age detection of fingerprints have to be researched in detail. First evaluations of the differential age detection show already promising results that should be confirmed using large scale tests.

Acknowledgments. The work in this paper has been funded in part by the German Federal Ministry of Education and Science (BMBF) through the Research Programme under Contract No. FKZ: 13N10818, FKZ: 13N10820, FKZ: 13N10822 and FKZ: 13N10821.

References

1. Leich, M., Ulrich, M., Hildebrandt, M., Kiltz, S., Vielhauer, C.: Forensic fingerprint detection: Challenges of benchmarking new contact-less fingerprint scanners – a first proposal, In: Pattern Recognition for IT Security. Darmstadt: TU-Darmstadt (2010).
2. Data Protection Directive 95/46/EC, Council of Europe Convention ETS no. 108; also OECD Guidelines 1980, UN Guidelines 1990; in Germany, since BVerfGE 65, 1.

3. Jain, A., Feng, J., Nagar, A., Nandakumar, K.: On Matching Latent Fingerprints, In: Computer Vision and Pattern Recognition Workshops, CVPRW '08, IEEE Computer Society Conference on, pp 1-8 (2008)
4. Lin, S.-S., Yemelyanov, K. M., Pugh, E. N., Engheta, N.: Polarization- and Specular-Reflection-Based, Non-contact Latent Fingerprint Imaging and Lifting, In: Journal of the Optical Society of America A, vol. 23, issue 9, pp. 2137-2153 (2006)
5. Jain, A., Chen, Y., Demirkus, M.: Pores and Ridges: fingerprint Matching Using Level 3 Features, 18th International Conference on Pattern Recognition, ICPR '06, pp. 477-480 (2006)
6. Popa, G., Potorac, R., Preda, N.: Method for fingerprints age determination, In: Romanian Journal of Legal Medicine, Vol 18, Issue 2, June 2010, pp 149-154, (2010)
7. Engel, A., Masgai, G.: Detektion von Fingerspuren und Windows-Fingerprint-GINA. Entwurf, Implementierung und Evaluierung, Bachelor Thesis, Otto-von-Guericke-University of Magdeburg, 2004.
8. Dubey, S. K., Mehta, D. S., Anand, A., Shakher, C.: Simultaneous topography and tomography of latent fingerprints using full-field swept-source optical coherence tomography, Journal of Optics A: Pure and Applied Optics, vol. 10, no. 1, pp. 015307–015315, (2008).
9. Kuivalainen, K. Peiponen, K.-E. and Myller, K.: Application of a diffractive element-based sensor for detection of latent fingerprints from a curved smooth surface, Measurement Science and Technology, vol. 20, no. 7, Page 077002, (2009).
10. EVISCAN by cote:m. [Online]. Available: http://www.cotem.de/eviscan_web/index.html (2010)
11. Chromatic White Light Sensor CWL - Fries Research & Technology - FRT GmbH. [Online]. Available: http://www.frt-gmbh.com/en/products/sensors/cwl/ (2010)
12. Singh, M., Singh, D. K. and Kalra, P. K.: Fingerprint separation: an application of ICA, Proc. SPIE 6982, 69820L (2008)
13. Chen, F., Feng, J. and Zhou J.: On Separating Overlapped Fingerprints, Biometrics: Theory Applications and Systems (IEEE BTAS 2010), pp. 1-6 (2010)
14. Tang, H.-W., Lu, W., Che, C.-M., Ng, K.-M.: Gold Nanoparticles and Imaging Mass Spectrometry: Double Imaging of Latent Fingerprints, Anal. Chem. vol. 82, no. 5, pp. 1589-1593 (2010)
15. Art. 16 Treaty on the Functioning of the EU; in Germany lately, BVerfG, 2 BvR 1372/07 (Mikado), para. 18.
16. Article 29 Data Protection Working Party of the EU: Biometrics (WP80), http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf, 2003, p. 5.
17. Article 29 Data Protection Working Party of the EU: Concept of personal data (WP136), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf
18. European Court of Human Rights, *S and Marper v. UK* (30562/04, 30566/04), para. 101.
19. BVerfGE (Collection of Federal Constitutional Court descisions, http://www.servat.unibe.ch/dfr/) 120, 378 (428).
20. BVerfGE 120, 378 (402); BVerfG, 2 BvR 1345/03 (IMSI-Catcher), Abs. 65; BVerfGE 115, 320 (342); BVerfGE 115, 166 (188); BVerfGE 113, 29 (46); BVerfGE 65, 1 (42).
21. Dix in: Roßnagel, Handbuch Datenschutzrecht, München 2003; Bygrave, http://www.austlii.edu.au/au/journals/UNSWLJ/2001/6.html, para. 20; Regan: Legislating Privacy, University of North Carolina Press, 1995, pp. 230ff.; Steinmüller, Informationstechnologie und Gesellschaft, Darmstadt 1993, p. 671; Podlech in: Brückner/Dalichau, Festgabe für Hans Grüner, Percha 1982, pp. 452ff.; BVerfGE 65, 1 (43); "scatter," BVerfGE 120, 378 (402 f.) w. f. r.
22. Hornung/Desoi/Pocs in: Brömme/Busch, BIOSIG 2010. Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, Bonn 2010, p. 83.
23. BVerfG 1 BvR 256/08, 2 March 2010, para. 224, http://www.bverfg.de/pressemit teilungen/bvg10-011en.html (English press release under "Data Security.").