Legally compatible design of digital dactyloscopy in future surveillance scenarios

Matthias Pocsa\textsuperscript{a}, Maik Schott\textsuperscript{b}, Mario Hildebrandt\textsuperscript{b}

\textsuperscript{a}Project Group Constitutionally Compatible Technology Design, University of Kassel, Wilhelmshöher Allee 64–66, 34109 Kassel;
\textsuperscript{b}Department of Computer Science, Otto von Guericke University, Universitätsplatz 2, 39106 Magdeburg, Germany

ABSTRACT

Innovation in multimedia systems impacts on our society. For example surveillance camera systems combine video and audio information. Currently a new sensor for capturing fingerprint traces is being researched. It combines greyscale images to determine the intensity of the image signal, on one hand, and topographic information to determine fingerprint texture on a variety of surface materials, on the other. This research proposes new application areas which will be analyzed from a technical-legal viewpoint. It assesses how technology design can promote legal criteria of German and European privacy and data protection. For this we focus on one technology goal as an example.

Keywords: Encryption, security, legally compatible technology design, privacy, data protection, digital capture of fingerprints

1. INTRODUCTION

One of these new applications is the surveillance application of the routine scanning of fingerprints on luggage at the airport in order to establish suspicious behavior or identify known criminals shows that due to the development of new sensors, information can be captured by automatic means in new situations of everyday life. In consequence, the police and private security services can observe and check a large number of persons. This increase of police observation creates opportunities and risks for society. Therefore it is necessary to design technology by taking the law into account. This is not only relevant for the design of the new sensor which acquires images but also the interaction with connected systems such as existing database systems storing reference data with which the acquired data is compared.

While the surveillance application will not be realized in the short term, apparently, fundamental rights will be involved in the future. To ensure protection of fundamental rights, this paper shows proposals for a system design that is compatible with high-level legal requirements. This paper focuses on a technology goal as an example for technology design that can promote compatibility with the law. Using German constitutional law and European fundamental and human rights as an example, this paper aims at raising awareness of the privacy impact of multimedia systems on society and fostering responsible technology development in the photonics research and application communities.

This paper develops a technology design goal whereby captured data are double encrypted and one key set is stored with the police, the other key set with the data protection authority (DPA). The motivation of this paper is to show how expensive the necessary security measures are for this particular application. Therefore the conclusion will hint at alternatives to that application which significantly improves legal protection.

2. SURVEILLANCE APPLICATION OF DIGITAL DACTYLOSCOPY

A certain surveillance application will serve as an example to illustrate the following technical-legal analysis. In that application fingerprint traces are scanned from luggage during luggage-handling at the airport (for details see [3], section 5.2). These traces are scanned prior to the departure of the airplane. If it becomes necessary to check the data, one searches these data on already known data from a database (of contact persons, criminals, or similar). In any case the captured data are strictly secured and deleted as soon as the airplane landed. If during the flight it gets known that an organized criminal, the airplane is put at risk or similar event takes place, the data are revealed for further investigation.
The data are earmarked accordingly. This application aims at gaining hints to detect terrorist and other networks by means of identification of persons.

Another application makes use of basic technologies that are currently developed. These new basic technologies for digital fingerprint capture are “Coarse Scan,” “Aging” and “Separation” [3]. The mere fact that a fingerprint trace is located at a position on luggage scanned where it was not before, can indicate suspicion or danger. This means for the surveillance application: During luggage handling at the airport, all fingerprint traces on bags are scanned, once before luggage handling and once afterwards. Then, only the numbers of the fingerprint traces are compared. If there are more traces afterwards there is reason to believe that the luggage was manipulated in the security zone of the airport. In variation of this it is possible that one will be able to establish the age of the fingerprint trace to find out whether there was manipulation during the luggage-handling. This technology application offers opportunities of detecting dangerous persons. However it also creates risks for the personality of individuals and the society at large. A solution could be a technique where the captured data are encrypted double and one of the two key sets is exclusively stored with the data protection authority. For such a four eyes principle at the institutional level another paper proposed technical measures [7]. Accordingly the police possesses (having applied so-called Biometric Template Protection [11]) no fingerprint images but only so-called pseudoidentifiers which entails two significant legal advantages: it is practically impossible to use biometric data as uniform identifiers and evaluate excessive additional information. However this approach is not useful for the technology that is assessed in this paper, that is, if in the end the police need the actual fingerprint trace image instead of pseudoidentifiers. This is due to the fact that with this technology fingerprint trace images are captured but biometric features are not extracted from them which would allow an automatic comparison of fingerprints. Nevertheless this restriction of automation also entails a significant legal advantage: it avoids the massive comparison of passengers’ fingerprints with the entirety of fingerprints of persons wanted by the police.

3. TECHNICAL AND LEGAL RISKS OF DIGITAL FINGERPRINT CAPTURE

As mentioned above the deployment of the technology offers opportunities of detecting dangerous people but also entails risks. The risk identification and evaluation usually builds on experiences already gained with the technology deployment. Since however no one has documented experiences with the specific technology application, this section goes on from general experience and for itself identifies the specific risks. The identification and evaluation of specific risks serves to develop appropriate measures to mitigate risks. Specific risks can therefore also necessitate that security measures that were only specified in computer science, now also need to be specified by law. This is because a technology application, to which so many people are exposed, does not only entail IT security risks but also societal and legal risks. Conversely this paper does not demand technical measures that would be possible but are not legally necessary. This technical-legal intersection is dealt with in this paper.

Confidentiality: In IT security the main goals are confidentiality (non-disclosure of data with respect to unauthorized entities), integrity (accuracy and completeness of data), authenticity (proof of the data’s origin (provenance) and genuineness or proof that an entity, like a person or other agent, has been correctly identified as originator, sender or receiver), non-repudiation (proof of the actual occurrence or non-occurrence of an event and its participating entities with respect to third parties) and availability (resources can be used and accessed by an authorized entity). Availability of infrastructure is not the main driver for this paper, but its loss can generally be mitigated by redundancy which is relevant to the legal criterion of system suitability mentioned below. These may be complemented by the legal requirement of privacy which is often used interchangeably with confidentiality. However, in a strict sense privacy refers to a person as such, whereas confidentiality refers to the data about the person, but also other non-personal data in general. The legal requirement is to only make use of as less private data as needed in order to avoid any personal references. Such personal references are considered as impossible if their creation is too expensive. Confidentiality, integrity and authenticity can be achieved by cryptographic means, especially digital signatures. To achieve the avoidance of personal references, we use a double encryption in a way that one of the two sets of keys is kept by the police and the other is exclusively retained by a trusted third party (in our case, the DPA). Since law and technology both aim at protecting privacy, in the following, the risks for privacy are assessed.

One has to distinguish between the two surveillance applications. The surveillance application using “Coarse Scan” and “Aging” entails significantly less risks. This is because one fingerprint trace cannot be distinguished from another and risks for the personality of individuals can hence not materialize. In contrast the first surveillance application using detailed scans allows identifying known wanted persons. This also increases the risks for them and all other citizens that
are exposed to the system. However it also offers the opportunity to identify wanted persons. Therefore the risks for this surveillance application are analysed in detail.

**Sensitive data and identifiers:** The capture of fingerprint traces and biological characteristics is already very risky for privacy. This is due to the fact biological characteristics reveal excessive additional information about illnesses, ethnic origin, etc. (sensitive data) and can act as access keys to connect several databases and captured data creating a profile as they are universal and life-long identifiers as well as coupled with location data.

“*False hits:*” Furthermore there is a risk caused by the statistic errors involved in comparison of biological characteristics. As soon as fingerprint traces are compared by the police with fingerprints of wanted persons, people could be confused with terrorists or other criminals.

**Erroneous operation:** In addition there is the risk of erroneous operation of the fingerprint system by police officers and other operators.

“*Function creep:*” Moreover there is the risk of “function creep.” The purpose of the data capture could be changed after the fingerprint systems have been introduced using the fight against serious crimes as a justification. Subsequently, ministers and senior police officers could urge parliaments to pass laws to use the system for punishing minor offences or taking measures against noncriminals like witnesses, contact persons, etc. The AFIS of the Bundeskriminalamt (Federal Criminal Police Office) contains fingerprints about four million people among which there are many that are not a terrorist or a similar criminal.

**Technology compliance:** Apart from that there is the risk of procuring and using a noncompliant fingerprint system. Fingerprint trace capture for police purposes is secret and automatic capture involves a large number of innocent people. Further the procurement and production of the technology is difficult because of the fragmentation of the EU security markets, lack of EU wide standards, fragility of the EU industrial base, and integration of societal aspects in the development of security technologies [5]. Therefore there is an increased need for checking whether or not the system design was analyzed and risks involved were mitigated and the system ensures pseudo-/anonymisation of captured fingerprint traces and IT security.

**IT security:** In addition there is the threat to IT security. A minister or senior police officer could “attack” the fingerprint system in order to achieve a successful result of a search. Even such illegitimate aims, the law needs to consider ([4], 208).

**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. Due to the risks of function creep, attacks by senior police officers, and erroneous operation of the fingerprint system, one could be exposed to police measures and this applies to a large number of innocent citizens due to the “high scatter” of the data processing. Hence citizens may feel like being watched and may abstain from deviant behavior. This does not only harm personality of individuals but also society at large. Those who abstain from deviant behavior may also abstain from being engaged in community life and committed to participating in political decision-making.

**Public safety paradox:** Finally there is the risk that the reliance on the fingerprint system could have negative effect on the overall public safety/security. Security officers that were in charge for the airport security could assume infallibility of the fingerprint system and act negligently. This could be dangerous because the terrorists and other criminals can avoid fingerprints or destroy system functions that allow identification of wanted persons.

### 4. FUNDAMENTAL RIGHTS IMPLICATIONS OF THE POLICE TECHNOLOGY

Due to the specific risks of the technology, there are serious implications for the fundamental right to “informational self-determination” according to the German constitution and the fundamental right to data protection according to EU fundamental rights. These rights provide for legal requirements that the fingerprint system has to meet. In order to meet the legal requirements this paper seeks to “translate” legal requirements into technology design. To this end it applies the method of German legal science called “KORA” (“Konkretisierung rechtlicher Anforderungen” = “Concretizing legal requirements”) [8]. This method is not only applicable to German law but also EU law and requires to develop (1) legal requirements from the legal settings - for the sake of brevity, this step is not included in this paper - (2) legal criteria from the legal requirements, (3) technology goals from the legal criteria - this paper deals with one technology goal - and finally (4) technology design proposals from the technology goals. This section outlines the legal criteria for technology
design that are supported by the case law of the Bundesverfassungsgericht and European Court of Human Rights, the provisions of the European Data Protection Directive and Bundesdatenschutzgesetz [9].

One has to distinguish between the two surveillance applications. The surveillance application using “Coarse Scan” and “Aging” offers advantages from a legal point of view [10]. Coarse Scans limit the pixel resolution of the captured image. Accordingly, one can only roughly see whether or not there is a fingerprint trace at a certain position of the luggage scanned - a “region-of-interest.” However, the image’s resolution is so low that one fingerprint trace cannot be distinguished from another. This same applies to “aging.” In contrast the first surveillance application using detailed scans allows identifying known wanted persons. This however comes with strict legal requirements that may be expensive. The following illustrates the extent of the legal requirements for the surveillance application using detailed scans.

**Transparent system design:** The system needs to be designed in a transparent way. Transparency enables courts and supervisory authorities to understand when and which police department used certain data in the past.

**System suitability:** The system needs to be able to achieve the stated goal of detecting criminals. For this one has to consider the technical possibility as well as the economic reasonability. This criterion enables that the data are available to the police when they need them and to the right police department(s).

**Use limitation:** The system needs to limit the data use to the stated purpose. This criterion disables the legislator to permit secondary uses of the IT systems procured for the fight against crime.

**Data security:** The system needs to be secured by technological means considering access controls and the state of the art (of cryptography). This is also a new requirement of Art. 27 of the Directive Proposal for Police Data Protection (it enshrines a list of access controls as legal requirements. Due to data security, one can trust in the police and DPA using the data in accordance with the law.

“The system needs to be designed in a way that the system administrator is a separate institution from the system users. The competent institution acts as the system user and has the sole power over the data, and the technical institution (“technisches Substrat” ([4], 211)) acts as the administrator who has the sole power over the data use as well as the program use ([4], 213). The current Data Protection Directive allows such joint controllership and this was therefore laid down in the Data Protection Act of the Land of Mecklenburg-Western Pomerania [6]. It is also provided for, as a new requirement, in Article 24 of the Data Protection Regulation Proposal of the EU Commission of January 2012 (COM(2012) 11 final of 25.1.2012). More progressively than the criterion of transparency, system protection enables the system administrator (e.g. DPA) to decide when and how the system user (e.g. police department) can use the system.

**Privacy by Design:** The system has to be designed in a way that unneeded personal data are not collected or are pseudo-/anonymized. This criterion removes or at least reduces all the specific risks (of using sensitive data, uniform identifiers, function creep, IT security, follow-up measures and the safety paradox).

**Accountability:** The system user needs to demonstrate that s/he has taken the measures to ensure data security and Privacy by Design. Further the user must 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. This criterion ensures that the technology design required by the law and the actual technology design correspond.

**Uniform identifiers:** The system user must not use the fingerprint images as uniform personal identifiers. This rules out the possibility to connect several databases creating a personality profile which violates the legal criterion of use limitation.

**False hit rate:** The system needs to be designed in a way that false hits are reduced. Hence people are more likely to be treated as nonsuspects.

**Sensitive data:** Article 8 of the Data Protection Directive prohibits the use of information about health, ethnic origin, etc. The system user must not make use of sensitive data that can be gained from biological characteristics. In this regard these characteristics are used in accordance with the criterion of use limitation.

**Distinction between individuals:** The system user must distinguish between individuals - between people having committed minor offences and serious crimes, between suspects and nonsuspects as well as between people suspected on the basis of mere assumptions and facts. The latter two distinctions are new requirements of Articles 5 and 6 of the Data.
Protection Directive Proposal for Police and Criminal Justice (COM(2012) 10 final of 25.1.2012). The police focus on identifying serious criminals and do not expose any other person that is known to the police to follow-up measures.

Avoidance of high scatter: It should be avoided that a large number of persons is exposed to the system (“high scatter”). This is a legal criterion recognized by the Bundesverfassungsgericht for police surveillance measures. Due to a high scatter of data capture, people might feel like being watched and abstain from deviant behavior and if the high scatter is avoided this risk is at least reduced.

Instant erasure: The system should be designed in a way that non-hits are instantly and securely erased. This criterion follows the Bundesverfassungsgericht in that it recognizes that risks are significantly increased if data are automatically compared with a wanted list and a person is exposed to a “hit” that is communicated to a police officer.

Indiscriminate data processing: The routine data capture and later use does not differentiate normal situations from situations where for the police there is a reason to believe that there is a danger (indiscriminate data processing). According to the Bundesverfassungsgericht the processing has to be based on such reasons. This is similar to the criterion of distinction between individuals. However if distinction between individuals is not possible because the police only knows that the suspect is at a certain place at a certain time, at least, the individuals that are there outside that time period should be let alone.

5. TECHNOLOGY GOAL: TWO-OFFICES PRINCIPLE

In order to meet the legal criteria for the surveillance application using the Detailed Scan that are outlined in the previous section, this section focuses on a technology goal that ensures double encryption of the scanned fingerprint traces in a way that two public authorities – the police and the DPA – can only jointly access (from the police’s viewpoint: only in cooperation with the DPA) captured trace data. For the purpose of this paper we call this the “Two-Offices Principle” (in the following: “TOP”).

Basically a simple encryption is only hardly sufficient. This is not because of some technical risks but of organizational, or more general, human risks. As fingerprints are a biometric feature and an important part in criminal investigations since several decades any misuse is considered grave as described in the previous sections and seen from the legal requirements for their handling. As such it was also shown that even the risk of misuse by the police or other authorities must be mitigated. Therefore if there were only a single asymmetric encryption of the fingerprints with the public key of said authorities, after they have received them they can just decrypt and virtually have unlimited access to them in the sense that no independent instance is auditing access and proper use. Therefore such an instance must be included in the whole handling of the fingerprints, i.e. a four-eyes principle must be employed. Such an independent instance may be the data protection authorities, which, at least in Germany, already are enabled to audit other federal and state authorities with regard to privacy and related issues.

As illustrated in figure 1, such a four-eyes principle can be implemented by cryptography by employing a double encryption of the content to be protected so that it is effectively protected by two layers. Thus always two parties – the security and the data protection authorities (DPA) – are needed to get access the actual fingerprints.

Figure 1. The technology goal of the Two-Offices-Principle by means of double encryption.

The TOP further requires adding metadata to the captured fingerprints. The metadata needs to contain anonymous identifiers to allow referring to an individual flight (maybe even the seat on the airplane) where an event takes place that justifies the use of fingerprints for identification of involved wanted persons. This way the police can specifically request
the DPA to decrypt fingerprints relating to a certain flight and the DPA can control that the police only gets to see those fingerprints it specifically requested.

The double encryption can be implemented by means of one pair of sets of keys – one set for the police and one for the DPA – and also several pairs of key sets. The latter may be necessary e.g. if several police authorities or suborganizational units therein handle the fingerprints in the application scenario. However the question whether or not several police authorities (and DPAs) are involved depends on the specific application. Therefore the goal is to enable the handling of several sets of keys and thus the design needed in the individual case.

Another aspect of the double encryption is the order of the encryption and thus inversely also the order the data is decrypted. If the police are the first and the DPA is the second to decrypt the scanned fingerprint data the DPA has full access to the data. If the police are the second instance it is the instance having full access. Since only the police are the ones that need the fingerprint the second approach may be preferable. However there are other factors in the specific application so that the technology goal of the TOP supports both approaches.

In addition to the double encryption the TOP requires that not only the data can only jointly be accessed but also the programs, parameters and other factors of system administration.

The TOP promotes the legal criteria mentioned above.

*Transparent system design:* Although the data are collected and in principle made available, they are instantly made confidential by automatic double encryption. The fingerprint traces can only be revealed if both authorities start to act jointly. This joint action necessitates that the police informs the DPA which creates transparency between the two authorities. This kind of transparency is particularly progressive because the police do not store the data themselves and only need to inform the DPA - this could be circumvented. Instead, they need to inform the DPA in order to receive the data. This effect deters the police in most cases from requesting data for unlawful uses and for the few cases where they need the data, transparency at least deters them from using the received data for secondary purposes because it can be detected.

*System suitability:* Availability of the fingerprint data is necessary for the system to be suitable to achieve the stated goal of detecting criminals. The TOP does as such not harm the achievement of this goal because the data remain available on occasions where the police can request the encryption key from the DPA. Quite the opposite, due to the TOP the encrypted data are no personal data anymore and can hence be made available to other police departments and in so doing further promote the detection of criminals. However the legal criterion of system suitability also needs to be assessed when specific technology measures for implementation of this goal are developed in the next section of this paper.

*Use limitation:* Since the captured data are instantly encrypted they cannot be used for any purpose. The TOP requires the use of anonymous identifiers for the fingerprint data to distinguish between each flight. This way the DPA can make sure that only the fingerprint data relating to a certain flight are decrypted. This promotes use limitation. There is only a residual specific risk that the DPA is requested to release decryption keys in relation to minor offences due to the imprecision of the law regulating the TOP.

*Data security:* The goal of the TOP promotes data security with regard to the fingerprints because double encryption is used that are stored in separate institutions’ systems. This means that an attacker is will not be successful in targeting one of these institutions’ information systems. This can only help removing one layer of encryption; however two layers need to be removed in order to access the fingerprint data. There is a residual specific risk that the DPA is deceived or negligent and sends the encryption keys to the police or another person who can too access the police system. Another risk with regard to data security - similar to use limitation - is that the respective security authority ultimately gains access to an unencrypted fingerprint and this fingerprint may be leaked due to insider or outsider threats. This cannot be avoided by technology alone because human knowledge and use is necessary. However one can restrict the number of people that are granted access to the data. One has to specify operational purposes and tasks in order to define personal user rights for the system. Further the measures of data security need to continuously reflect the state of the art. Thus in relation to the user rights, this legal criterion is relevant to the measures developed in the next section of this paper. Further - like for system suitability - the goal promotes data security because it improves availability of the stored data.

“System protection:” Likewise the legal criterion of “system protection” is promoted by the technology goal. Although it is not the system administrator and the system user that are two separate institutions but these two separate institutions share the functions of system use and system administration. This means that neither institution can use or change the
system alone. Due to this functional similarity one can argue that this legal criterion is satisfied. Like “progressive” transparency, system protection deters the police from unlawful data request and secondary data uses.

*Privacy by Design:* The TOP promotes Privacy by Design because the encrypted data can only be decrypted by means of participation of the DPA. This can be regarded as pseudonymisation or even anonymisation (since no-one can alone decrypt the data).

*Accountability:* The goal of enforcing the TOP does as such not demonstrate that the system user has taken the measures for compliance. However the TOP cannot be realized without proper mechanisms to implement the sophisticated technology design and architecture. The measures need to be specified in a sufficiently precise manner in order for their effectiveness to be verifiable by an auditor. This will be done in the next section of this paper.

*Uniform identifiers:* Since the captured data are instantly encrypted they cannot be used for any purpose (see above) which makes it all the less likely to use the fingerprint images as uniform identifiers.

*False hit rate:* The encryption prevents the police from using the fingerprint images to compare them with AFIS or other reference databases. Hence the technology goal reduces false hits.

*Sensitive data:* Since the captured data are instantly encrypted they cannot be used for any purpose (see above) which makes it all the less likely to make use of sensitive data that can be gained from biological characteristics.

*Distinction between individuals:* The goal of the TOP cannot promote the distinction between individuals. This is due to the fact that such distinction mainly depends on the design of the reference database. The technology goal in this paper refers is restricted to the capture of fingerprint traces.

*Avoidance of high scatter:* The TOP avoids a high scatter because instead of the fingerprints of all flight passengers only the ones relating to a certain flight belong to an identifiable person.

*Instant erasure:* The TOP makes personal fingerprint data - the raw data - superfluous. However the raw data need to be instantly and securely erased in order to promote the legal criterion of instant erasure. This will be developed in the next section of this paper.

*Indiscriminate data processing:* The technology goal can avoid indiscriminate data processing because the police only possess personal data in case that they can request data from the DPA. Hence the data processing can be reduced to situations where for the police there is a reason to believe that there is a danger and individuals that are there outside that time period are let alone.

### 6. TECHNICAL AND ORGANIZATIONAL MEASURES

As shown in the previous section the technology goal of the TOP satisfies most legal criteria derived from the fundamental rights impacted by the fingerprint application. In order to achieve the technology goal this section suggests specific measures of technology design. As mentioned above these measures are limited to the legally necessary and they aim at keeping the encryption key of one authority confidential in relation to the other authority.

In order to achieve the technology goal the whole lifecycle of the scanned fingerprints must be considered. This starts with the creation of the fingerprint scan or the digitalization of the fingerprint by using some kind of sensor which results in a fingerprint image. For this purpose most likely off-the-shelf sensor will be used (promoting the legal criterion of *system suitability* because specially developed technology could be too costly), which means that they won’t employ special precautions to prevent misuse of the scans, i.e. by encrypting them on the fly during the digitization process (violating *all the other legal criteria*). As such it can be assumed that at least at this time and immediately after the digitization process a raw unprotected digital copy of a fingerprint exists. Thus several measures must be employed to avoid any use of fingerprint data before the double encryption, that is: a) the timespan until the encryption must be as short as possible; b) after encryption the unencrypted fingerprint must be removed without any means for recovery, i.e. by securely erasing the fingerprint or, preferably, never have been stored on a hard-disk but residing in memory only and then overwritten; and c) the digitization device and any other system parts having direct access to it must be considered as high-security, i.e. very restrictive access technical and organization policies must be in place for this system, e.g. the system must not be accessible by systems of a lower security level or by unauthorized persons. These measures for shortening the timespan, nonrecoverability and “high security” promote the legal criteria of *data security, Privacy by Design* and *instant erasure*.
Aside from the kind of encryption to be used which is tackled in detail later, first the storage of such encrypted fingerprints is considered. Considering our application scenario, where a large amount of fingerprints – one for each passenger – needs to be stored, databases may be used for this purpose. The fingerprints are stored for the time of the passengers’ travel and some retention time beyond, but much shorter than the valid time of used encryption algorithm for the used parameter set, especially the keylength. There exist several recommendations of which encryption algorithms with which parameters are considered secure until a specific time, like the US NIST [1] recommendations or the German BSI recommendations [2]. For example as January 2012 the latter recommends RSA2048 with certain requirements as secure until 2018. Although this may and possibly will change to an earlier date due to advances in cryptography such timespans can be considered much longer, than the timespan the fingerprint are stored inside the database. This also holds true in case an algorithm gets broken, which does not happen out of the blue but is normally preceded by theoretical attacks which lower the trust in the algorithms much earlier. As such for our application scenario the risk can be considered low that the encrypted fingerprints get broken during their lifetime in the database assuming short retention times. The strength of the encryption with regard to the short retention period promotes the legal criteria of use limitation and data security including the state of the art.

A more grave issue is the time period after the retention time. The result is that the encrypted fingerprint must be erased in a secure manner. However, this is not a trivial matter in the case of databases due to their transparent way to store data, i.e. one usually only has logical access to the data but no physical access to where the data is actually stored which may even be done using a distributed storage. Therefore precautions must be taken to use a databank system having means to securely erase data or providing physical access to the data. These measures for secure deletion of the encrypted fingerprint data promote the legal criterion of data security.

The security deletion also refers to the private keys to mitigate the risk of misuse, which increases with the count of used keys, including that it can be expected that for private keys that are not used anymore their proper custody may grow laxer in time. Additionally, in the instant a private key is securely deleted, all encrypted data meant to be decrypted by it automatically also becomes unavailable. However, as described this only holds true until the specific algorithm used for encrypting gets broken. Nevertheless, the confidentiality of the data increases with the loss of the respective private key.

Encrypting the fingerprints is the crucial means to protect them and such is described in more detail in the following. The important question at this point is about the order of the encryption and thus inversely also the order the data is decrypted.

Considering the content C shall by encrypted using an encryption function E and a decryption function D we have \( C' = E(K_{pub}, C) \) and \( C = D(K_{priv}, C') \), whereas \( K_{pub} \) is the public key of the recipient needed for encryption and \( K_{priv} \) the respective private of the recipient at his side needed for decryption, whereas \( K_{pub} \neq K_{priv} \), i.e. asymmetric encryption must be used. With two instances we also have two sets of such key pairs: \( K_{pub,Sec} \) and \( K_{priv,Sec} \) for the appropriate security authorities and \( K_{pub,DPA} \) and \( K_{priv,DPA} \) for the data protection authority. \( K_{pub,Sec} \) and \( K_{priv,Sec} \) may each be a set of keys, one for each security authority or suborganizational unit therein that may handle the fingerprints in the appropriate application scenario. Thus each of them may independently decrypt the respective encryption layer for the security authorities. This promotes the legal criteria of system suitability and data security due to the redundant availability to several police authorities, departments, etc. Basically, the same also holds true for the data protection authorities. However it may be preferable to task only one data protection authority with controlling the access to the fingerprints as it must always be known which security authority has requested and has been granted access to each fingerprint, which may become difficult if such information is handled by different data protected agencies. This may harm the legal criterion of use limitation. On the other hand one may argue that multiple data protection agencies could synchronize their respective records, which may also serve as a kind of many eyes principle between themselves (if it is assumed that the DPA has truthfully and completely distributed the records for synchronization beforehand). This supervision of the supervisor promotes use limitation. Both cases may be legally preferable. Additionally, in a strict technical sense encrypting a message in such a way that multiple recipients can receive it, is usually done by symmetrically encrypting the message with a randomly generated key, then asymmetrically encrypting this random key with the public key of all recipients and attach this encrypted key to the encrypted message. As such any of the recipients can decrypt this random key with its private key and use it to finally decrypt the message.

For the sake of brevity without loss of generality we handle this in the following that only one security and data protection authority is involved, which may actually stand for a set of them, as well as that only one encryption and decryption method E and D – each implying the step with symmetric random key – is used for both parties although both parties may be using different kinds of algorithms and parameterizations. Additionally, the intersection \( K_{pub,Sec} \cap \)
$K_{\text{pub,DPA}}$ must be $\emptyset$, i.e. the used public keys for each layer must not have one common key included as this would allow a single entity to decrypt both layers at once. This must not be restricted to the keys itself but also to the participating organizations in the sense that no organization must have the ownership of or other access to a private key which is used by the data protection authorities and at the same time have access to another private key used by the security authorities.

As encryption and decryption keys, one can use certificates or signatures according to the Signaturgesetz (German Signature Act) and national implementations of the EU Signature Directive. In line with these laws infrastructures have been created that allow the use of trustworthy signatures. Since they are already created the TOP does not entail additional costs creating such infrastructure. This promotes the legal criterion of *system suitability* and *Privacy by Design* because it avoids undue costs.

Furthermore the security of the key pairs needs to be ensured. Integrity or authenticity issues of a key result virtually in its non-availability. In the encrypting system, i.e. the system where the fingerprints are digitized and encrypted, this refers to the deposited public keys of the DPA and security authorities. Thus if either the public key of the DPA or the security authorities is not available the double encryption cannot take place. However, this may be mitigated by not only having one key for the DPA and one for the security authorities, but several keys. As a private key should only be present at one location – to reduce the risk of its disclosure – and a private key also is some kind of identification, each organizational unit that needs to partake in this application scenario needs their own private key and thus own public key. Therefore it is to be assumed that multiple public keys are present which are usable to encrypt the fingerprints. The same non-availability issues apply to the private key. It is crucial that they are stored with special care, i.e. access must be restricted, ideally password protected with symmetric encryption, and logged. If there are hints of the private key being copied or in general accessed by a non-authorized entity, the key pair must be revoked and new key pair needs to be created. The private key must then be deleted as early as possible. However, it must be noted that this does not has an impact on the fingerprints, due to their double encryption where they are still protected by the other layer. Of course, this only holds true if the disclosed private key does not get in the hands of one of the other parties of the other layer, which could then maliciously use this key to decrypt the whole fingerprint on its own. These measures for ensuring the security of the key pairs particularly promotes the legal criteria of *system suitability* and *data security*.

For both parties there are only two kinds of double encryption possible: a) $C'' = E(K_{\text{pub,Sec}}, E(K_{\text{pub,DPA}}, C))$ and $C = D(K_{\text{priv,DPA}}, D(K_{\text{priv,Sec}}, C'))$ if the first layer is removed by the security authorities and the second layer by the data protection authorities whereas afterwards the fingerprint is accessible (see figure 2); or b) $C'' = E(K_{\text{pub,DPA}}, E(K_{\text{pub,Sec}}, C))$ and $C = D(K_{\text{priv,Sec}}, D(K_{\text{priv,DPA}}, C'))$ the other way around were the data protected authorizes removes the first layer and the security authorities the second layer (see figure 3).

![Encryption and decryption workflow](image)

In the first approach (figure 2) the security authority requests a certain fingerprint. After it retrieves the fingerprint it can decrypt the first layer with its private key, but has no access to the actual fingerprint yet. For this it sends this to the data protection authority which then provides the final decryption. At the same time it can see and control which items the security authority actually requests and thus may even deny requests, e.g. if there are reservations with regard to the principle of proportionality. However this is not necessary because either way the DPA only sends the keys relating to a certain flight to the police so that only these fingerprint data can be further used. Moreover it contradicts the legal criterion of *use limitation* and *system protection* because the DPA does not have to know and use the actual fingerprints but only to ensure the proper knowledge and use by the police (system administration). Additionally the unencrypted fingerprint needs to be sent back to the originally requesting security authority which would include an additional step of encrypting and decrypting for this transmission only. This contradicts the legal criteria of *system suitability* and *data security* because it increases the required investment of work, time, and costs.
In second approach (figure 3) the requested fingerprint is first sent to the data protection authority by the requesting security authority. The first layer is decrypted and then the still (single) encrypted fingerprint can be sent normally back to the requesting security authority, which can now decrypt the final layer and access the fingerprint data for its task. Although the data protection agency cannot directly monitor what exactly was requested, this may not even be necessary if the appropriate metadata is part of the encrypted fingerprint, i.e. \( C'' \) consists of the encrypted fingerprint \( C' \) as well as anonymous identifiers about the fingerprint. Since the anonymous identifiers specify time and date of the fingerprint capture, the DPA can establish whether or not the encrypted fingerprints are related to the flight that is subject to the police investigation. The police will therefore only send the right sets of encrypted fingerprints to the DPA. Otherwise the DPA will know that these fingerprints are relating to other people and therefore delete them without sending these decrypted fingerprints back to the requesting police department.

Additionally the data protected authority knows which security authority asked them for a fingerprint, when they did ask, and why they did ask. This has then one great advantage: the fingerprint may be encrypted but ultimately the security authorities need a decrypted fingerprint to compare them with their criminal databases. Although they are obliged to remove unneeded data and only use them for the stated purpose, this may not always be happen, be it intentional or non-intentional. However, such intentional or non-intentional violations can be uncovered by using random examinations by the data protection authorities or during trials. If a random examination finds a certain fingerprint the security authority should be able to state where this fingerprint comes from (i.e. it should also have an anonymized identifier) and if it is a fingerprint from an earlier investigation using this identifier it can be traced back using the records of the data protected authority when and for what purpose this fingerprint was originally requested, thus uncovering misuse. The same may apply during trials if they are requested to state where the used fingerprint was originally obtained from.

Regarding “system protection” and derived from this “data security” two environments must be considered: the encryption systems – here at the site or in the domain of the airports – and the key generating and decryption systems at the data protection and security authorities.

Beginning with the latter, one risk may be a back-door placement of manipulated software used for key generation which then creates key pairs whose use allows the police (in case of the system of the data protection authorities) or a third party to decrypt messages. This is somewhat similar to the earlier mentioned requirement that one organization must not have access to a private key used by a data protection authority and another private key used by a security authority at the same time. This risk can be mitigated by generating the key pairs on an isolated system and employing the means described above like restrictive access rights and encryption. If the software used for key generation is updated, special care must be taken that it is acquired from official sources and by checking its integrity and authenticity using the provided cryptographic hashes or signatures. As access control mechanisms only limit read and write access, these permissions may be changed at any time by the system administration and can be circumvented by accessing the data without using OS functionality. If a system administrator tries to replace the encryption software by malicious software, the second system administrator can verify this by comparing the publically known hash of the software. Following the Two-Offices Principle here would not provide any benefit, as one side (either data protection or security authority) cannot harm the other side by manipulating its own software as the software only needs the basic functions of key generation and decryption. Neither provides a tweak of the generated keys an advantage nor does the decryption. The major issue is the leaking or exchange of the keys, which however only hurts the side where it happens. As such in this case a four-eyes principle is sufficient and even preferable over the Two-Offices Principle, which would here provide each side access to the other side.

On the other hand, this is different for the encryption systems. As it basically shares the same risks as described in the previous paragraph, the mitigation measures of being an isolated system, strict access control rights, and encryption of confidential data also apply. However, it also has a major additional or extended risk. This is that a manipulation of the software or the stored public keys, may lead to the case that at least one level of the message is encrypted with a key that

![Diagram of encryption and decryption workflow](image-url)
is owned by a party which must not be able to decrypt this level. For example, on the level of data protection authorities one used key is not one of the data protection authorities but of the security authorities, i.e., the condition: \( K_{\text{pub,Sec}} \cap K_{\text{pub,DPA}} = \emptyset \) is violated. The same applies for the key of a third party \( K_{\text{pub,3rd}} \) which was maliciously injected in the set of \( K_{\text{pub,Sec}} \) and \( K_{\text{pub,DPA}} \), as well as the data protection authorities injecting a key in the set \( K_{\text{pub,Sec}} \). However, one can consider the latter to be a lesser threat as the data protection authorities have no benefit in obtaining fingerprints and going lengths to manipulate system programs and system data. Thus, like in the previous paragraph the system administration should be done by a four-eyes principle at least, whereas the system need to be regularly audited by the data protection authorities or one of both system administrators is part of the data protection authorities. Critical data then needs to be (symmetrically) encrypted with a key from the data protection authorities. This Two-Offices Principle at the level of system administration fulfills the legal criterion of “system protection.” and promotes data security.

To sum up one can observe that the surveillance application of the digital fingerprint capture using Detailed Scans in order to identify known wanted persons are subject to strict legal requirements. Therefore the application needs to meet a lot of legal criteria. This leads to the fact that numerous and expensive technical and organizational measures need to be taken. Thus the legislator needs to decide whether it is worth it to allow the use of the digital fingerprint capture in that particular surveillance application. An alternative for the legislator to avoid this expensive technical implementation could be the digital capture of fingerprint traces using the basic technologies Coarse Scans and Aging for other surveillance applications.

7. CONCLUSION

The digital capture of fingerprints for crime prevention by means of detailed scans for the duration of a flight enables the police to identify wanted persons that have given reason for the police to believe that there is a danger. However this technology application is very risky for the fundamental rights of all other passengers. Therefore the police need to take very sophisticated measures to ensure the Two-Offices Principle - as shown in this paper. Further the description of the measures of technology design in this paper and the impact assessment throughout this paper are the basis for the system user to meet the legal criterion of Accountability. The measures of technology design and their effectiveness are verifiable by an internal or external auditor. This should therefore be included in the documentation which can then be included in the internal data protection policy required by the criterion of Accountability.

Nevertheless the sophisticated measures that need to be taken are very expensive. Therefore the photonics and security research communities should head a certain direction. New basic technologies such as the “Coarse Scan” of fingerprints and fingerprint “Aging” are suggested [3]. These could replace the detailed scan of fingerprints. These basic technologies do not allow identification of wanted persons, however, one can identify luggage that is manipulated during the luggage-handling. Such technology applications could significantly improve crime prevention at the airport.

REFERENCES


