



FIDIS

Future of Identity in the Information Society

Title: “D6.1: Forensic Implications of Identity Management Systems”

Author: WP6

Editors: Zeno Geradts (NFI, The Netherlands)
Peter Sommer (LSE, UK)

Reviewers: Martin Meints (ICPP, Germany)
Mark Gasson (University of Reading, UK)

Identifier: D6.1

Type: [Deliverable]

Version: 1.0

Date: Monday, 09 January 2006

Status: [Final]

Class: [Public]

File: FIDIS_WP6_1_final.doc

Summary

The objective of this document is to provide an overview of the forensic implications of current Identity Management Systems. Because of the broad scope of this field, this document should be viewed as a guide and does not attempt to be entirely comprehensive. In-depth examples of biometric devices and mobile networks are given in the forensics context. An overview of legal systems is also provided with a comparison of digital evidence law in different countries. From the examples used and the legal systems considered, the general conclusion is that forensic information can be extracted from many electronic devices and can subsequently be used in court. However, in the examination process, it is important to consider the likely integrity of the data, i.e. how failsafe the retrieval system is, since this will undoubtedly have an impact on the identity of the real person involved as a suspect. Equally, it is necessary to ensure law enforcement investigators and technical analysts follow the necessary protocols such that otherwise admissible electronic evidence is not suppressed or legally compromised.



Copyright Notice:

This document may not be copied, reproduced, or modified in whole or in part for any purpose without written permission from the FIDIS Consortium. In addition to such written permission to copy, reproduce, or modify this document in whole or part, an acknowledgement of the authors of the document and all applicable portions of the copyright notice must be clearly referenced.

The circulation of this document is restricted to the staff of the FIDIS partner organisations and the European Commission. All information contained in this document is strictly confidential and may not be divulged to third parties without the express permission of the partners.

All rights reserved.

<p><u>PLEASE NOTE:</u> This document may change without notice – Updated versions of this document can be found at the FIDIS NoE website at www.fidis.net.</p>
--

Members of the FIDIS consortium

1.	<i>Goethe University Frankfurt</i>	Germany
2.	<i>Joint Research Centre (JRC)</i>	Spain
3.	<i>Vrije Universiteit Brussel</i>	Belgium
4.	<i>Unabhängiges Landeszentrum für Datenschutz</i>	Germany
5.	<i>Institut Europeen D'Administration Des Affaires (INSEAD)</i>	France
6.	<i>University of Reading</i>	United Kingdom
7.	<i>Katholieke Universiteit Leuven</i>	Belgium
8.	<i>Tilburg University</i>	Netherlands
9.	<i>Karlstads University</i>	Sweden
10.	<i>Technische Universität Berlin</i>	Germany
11.	<i>Technische Universität Dresden</i>	Germany
12.	<i>Albert-Ludwig-University Freiburg</i>	Germany
13.	<i>Masarykova universita v Brne</i>	Czech Republic
14.	<i>VaF Bratislava</i>	Slovakia
15.	<i>London School of Economics and Political Science</i>	United Kingdom
16.	<i>Budapest University of Technology and Economics (ISTRI)</i>	Hungary
17.	<i>IBM Research GmbH</i>	Switzerland
18.	<i>Institut de recherche criminelle de la Gendarmerie Nationale</i>	France
19.	<i>Netherlands Forensic Institute</i>	Netherlands
20.	<i>Virtual Identity and Privacy Research Centre</i>	Switzerland
21.	<i>Europäisches Microsoft Innovations Centre GmbH</i>	Germany
22.	<i>Institute of Communication and Computer Systems (ICCS)</i>	Greece
23.	<i>AXSionics AG</i>	Switzerland
24.	<i>SIRRIX AG Security Technologies</i>	Germany

Versions

Version	Date	Description (Editor)
0.1	01.12.2004	<ul style="list-style-type: none">• Initial release (Peter Sommer)
0.2	01.05.2005	<ul style="list-style-type: none">• Corrections by Mieke Loncke after review from Zeno Geradts
0.3	01.08.2005	<ul style="list-style-type: none">• Zeno Geradts: all contributions are added, some global text is added and intro and conclusions with editing GSM of Falk Wagner / edited by Zeno
0.4	09.09.2005	<ul style="list-style-type: none">• Changes following first internal review by Martin Meints. Chapters 9 and 10 to be processed by their authors.
0.5	13.09.2005	<ul style="list-style-type: none">• Chapter 10 introduction and conclusions added. Chapter numbering updated.
0.6	15.09.2005	<ul style="list-style-type: none">• Major formatting changes, correction of usage and syntax and additions throughout. Chapter numbering redone.
0.7	26.09.2005	<ul style="list-style-type: none">• Corrections following internal review by Mark Gasson.
0.8	30.09.2005	<ul style="list-style-type: none">• First version for second internal review.
0.9	15.12.2005	<ul style="list-style-type: none">• Minor corrections following second internal review.
1.0	12.01.2006	<ul style="list-style-type: none">• Final version

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

Chapter	Contributor(s)
All Chapters	Peter Sommer (LSE, UK), Zeno Geradts (Netherlands Forensic Institute, The Netherlands)
Chapter 4	Falk Wagner, (Goethe University Frankfurt, Germany)
Chapter 5	Rikkert Zoun, (Netherlands Forensic Institute, The Netherlands)
Chapter 6	Mieke Loncke, (University of Leuven, Belgium)
All Chapters	Martin Meints (ICPP, Germany), Mark Gasson (University of Reading, UK)

Table of Contents

1 Executive Summary 9

2 Introduction..... 10

 2.1 Scope..... 10

 2.2 Objective 10

 2.3 The content and structure of this document 10

3 Describing forensic aspects of ID systems 11

 3.1 Taxonomy 11

 3.2 Deriving a model of forensic aspects 11

 3.2.1 An overview of the artefact..... 11

 3.2.2 Threat level..... 14

 3.2.3 Forms of failure 14

 3.2.4 Verification problems 16

 3.2.5 Consequences of failure..... 17

 3.2.6 Forensic aspects..... 18

 3.3 Conclusion 19

4 Case study: Reliability of Identification in Mobile Phone Networks 20

 4.1 Introduction 20

 4.2 Applying the forensics model 20

 4.2.1 Threat levels 20

 4.2.2 Threats at Account Level 21

 4.2.3 Threats at a Technical Level 22

 4.2.4 Forensic reliability 24

 4.2.5 Forms of failure 25

 4.2.6 Consequences of failure..... 26

 4.3 Conclusion 27

5 Case Study: Biometric Artefacts..... 28

 5.1 Introduction 28

 5.2 Biometric artefacts used for identification and verification 29

 5.2.1 Overview 29

 5.2.2 Fingerprint..... 30

 5.2.3 Iris 33

 5.2.4 Hand geometry 34

 5.2.5 Hand vein pattern..... 35

 5.3 Forms of failure of biometric systems..... 36

 5.4 Verification problems: biometric device technology 39

 5.4.1 Evaluated devices 39

 5.4.2 Image extraction using live fingers with various skin conditions 40

 5.5 Threat level of biometric device spoofing 45

5.5.1	Fingerprint spoofing	45
5.5.2	Iris spoofing.....	61
5.5.3	Hand geometry spoofing	62
5.5.4	Hand vascular pattern spoofing.....	65
5.6	Conclusion	69
6	Overview of case law and acceptance of electronic evidence in court.....	70
6.1	What is forensic evidence?	70
6.2	The collection of evidence	71
6.2.1	Admissibility of the evidence.....	71
6.2.2	A. Freedom of evidence	71
6.2.3	B. Legality of the evidence	72
6.2.4	C. Countries where evidence is even more restricted.....	72
6.3	The taking of samples	73
6.4	Admissibility of expert’s opinion in court.....	74
6.4.1	The risks inherent in forensic evidence	74
6.5	Reporting requirements.....	75
6.6	Admissibility standards	75
6.6.1	Frye	76
6.6.2	Daubert.....	77
6.6.3	Kumho.....	77
6.6.4	Other standards.....	78
6.7	Sanctions on evidence.....	78
6.8	Digital evidence.....	79
6.9	Cybercrime.....	80
6.9.1	EU: Convention on cybercrime (Council of Europe)	81
6.9.2	The Netherlands: the Computer Crime Act of 1993.....	82
6.9.3	Belgium: Computer Crime Act of 2001.....	83
6.9.4	United States: Computer Fraud and Abuse Act (CFAA) and the Electronic Communications and Privacy Act (ECPA)	83
6.10	Electronic signatures.....	84
6.10.1	European Union.....	84
6.10.2	United States	85
6.11	Impediments of digital evidence	85
6.12	Admissibility of digital evidence in court.....	86
6.13	Physical evidence	88
6.14	Non-biological evidence	89
6.15	Biological evidence – biometric identification	89
6.15.1	DNA profiling (also known as DNA fingerprinting)	90
6.15.2	Fingerprints	97
6.15.3	Handwriting identification	98
6.15.4	Voice identification (Speaker identification SPID).....	100

Future of Identity in the Information Society (No. 507512)

6.15.5	Ear print identification	100
6.15.6	Lip print identification	102
6.15.7	Facial recognition	102
6.15.8	Iris recognition and retina	102
6.15.9	Bite mark identification	103
6.15.10	Conclusion.....	103
6.16	Forensic Identification databases	103
6.17	Privacy and the use of databases	103
6.17.1	United States	104
6.17.2	European Union.....	104
6.18	Dangers?	108
6.19	Conclusion	108
7	Conclusion	109
8	Glossary.....	111

1 Executive Summary

In this document an overview of the different forensic aspects and implications of Identity Management Systems is given. This work is based on the joint FIDIS and European Network of Forensic Institutes (ENFSI) kick-off workshop (Krakow, September 2004) and thus includes input from a broad although not comprehensive range of partners. The focus here is on state-of-the-art technology, but does not attempt to be a comprehensive listing of all such Identity Management Systems.

In this document, a model has been derived as a basis to represent information pertaining to the forensic aspect of Identity Management Systems. This model is described in detail to highlight the key facets of this area. Additionally, using aspects of this model, the forensic implications of biometric systems and mobile devices, two case studies where forensic information can be extracted, are examined in depth. This document also describes a taxonomy concerning the different aspects of these systems related to forensic evidence in court, and gives an extensive overview of the impact of different legal systems on such 'digital evidence'.

The general conclusion that is drawn from this research is that evidence from identity based systems is legally permissible, and indeed heavily used in courts of law. For example, location information from Global System Mobile devices is frequently used for tracking individuals and subsequently for checking if associated statements made by suspects and witnesses with regard to their locations are correct. Similarly, supposedly unique biometric identifiers are becoming more frequently utilised to gain system access, and supposedly provide proof of a person's identity and thus accountability of subsequent actions.

However, with many of these systems there exists a possibility of incorrect association of a user with a mobile device, deliberate tampering with the system or system error through incorrect usage or technical faults. A classic example is that fingerprints can be spoofed, and indeed other biometric features can be copied, even without the owner of that feature knowing it. For this reason, in the examination process it is important to consider the likely integrity of the data, i.e. how failsafe the system is, since this could provide an alternative hypothesis, i.e. a different individual being involved in the crime. Equally, it is necessary to ensure law enforcement investigators and technical analysts follow the necessary protocols. In doing so, prosecutors can ensure that otherwise admissible electronic evidence is not suppressed or compromised legally either because of an illegal search and seizure or because the evidentiary foundation was not properly or credibly laid during trial.

2 Introduction

2.1 Scope

This document, created in the context of workpackage 6 of the **FIDIS Network of Excellence**, proposes to give an overview of forensic implications specific to Identity Management Systems.

The target of this document is both non-experts (citizens, employees, civil servants, ...), who need to have a quick understanding of the way that identity is managed in different application domains (and in particular what the categories of people's attributes that are dealt with or manipulated are); and experts who want to get a more global (multidisciplinary) understanding of the different models that are used to manage identity (in particular in those application domains they are less familiar with).

2.2 Objective

The objective here is to provide an overview of forensic implications relating to the practical use of identification systems. To clarify, the term forensic as defined by the Webster dictionary is:

- 1. Belonging to, used in, or suitable to the courts or to public discussion and debate*
- 2. Relating to or dealing with the application of scientific knowledge (as of medicine or linguistics) to legal problems (forensic pathology) (forensic experts) fo-ren-si-cal-ly, adj.*

The term forensic, as used in this report, refers to information that is used in court as evidence. Such information can be extracted from identification management systems. This evidence can be very strong, however some limitations are apparent. For example, one should always investigate whether it is possible to circumvent the system in such a way that it appears person X did a certain action, however in practice it was impostor Y. Notably, chapter 6.1 gives in detail an overview of forensic evidence from the legal point of view.

2.3 The content and structure of this document

This document is based on the results of a workshop involving FIDIS and the working group Forensic IT of the European Network of Forensic Institutes (ENFSI) in September 2004. The workshop resulted in a model which describes the forensic aspects of identification management systems which is described and explained here in Chapter 3. Also considered here in the forensics context are examples where the identification management system is implemented in some depth, for example mobile phone networks (Chapter 4) and biometric devices (Chapter 5).

Additionally, since digital forensic evidence is used in many different legal systems across the world, an overview of different legal systems is given in Chapter 6, examining how digital evidence is considered and utilised within them.

3 Describing forensic aspects of ID systems

3.1 Taxonomy

Although the aim of the kick-off workshop and subsequently this document was in part to produce a taxonomy of issues, it is apparent that there is a multiplicity of possible taxonomies.

Challenges to Identity Management Systems could be mounted on several grounds of which the following are simply illustrations:

- that the artefact of identity document, token, magnetic-stripe card, smart-card, etc – could be faked
- that a legitimate artefact of identity could be obtained by fraudulent means
- that a legitimate artefact of identity in the possession of its legitimate owner may contain misleading or inaccurate information
- that there was fraud or poor quality procedures within the body issuing the artefact of identity such that it was unreliable

3.2 Deriving a model of forensic aspects

Forensic scientists and investigators will generally look for material which exists but which was not necessarily designed to be retrieved and utilised as evidence. This material is termed “unintended audit trails”, and for example could be: Telecommunication records, cell site analysis; extended use of vehicle number plate recognition systems and so on. We have chosen a model as a basis to represent such information pertaining to the forensic aspect of Identity Management Systems:

1. an overview of the artefact
2. the threat level
3. forms of failure
4. consequences of failure
5. in conclusion: the forensic aspects

This model will be further elaborated below. The model has been chosen to structure the information.

3.2.1 An overview of the artefact

Many different artefacts exist which can be grouped together based on the technology they utilise. However, for the purposes of this work, during the kick-off workshop, the ENFSI-group and FIDIS participants discussed the following broad range of artefacts and grouped them accordingly:

3.2.1.1 Paper-based document

A traditional example is the passport and an id-card with non-digitally stored 'biometric' information such as signature, photograph, height and, in some countries, fingerprints, see section 3.2.1.4. This information is stored together with the names, place of birth and other information related to the document.

3.2.1.2 Magnetic-stripe

Magnetic stripe cards have been in use for several decades, with the credit card being a classic example. However, the magnetic stripe is known for the ease at which a copy can be made. Since convenience is particularly important when using these cards, magnetic stripe cards are still in use in the financial sector.

3.2.1.3 Smart-card

Smart cards were first introduced on a large scale as prepaid cards for public phones. Nowadays many people own their own mobiles, and so smartcards are often seen in these mobile devices as SIM cards (the chip-cards in the mobile phones). Furthermore, payment schemes are implemented on smart-cards. They are more difficult to copy and thus offer a more secure method for authentication, in many cases in combination with a pin-number. Nowadays the credit card companies are also implementing these systems in their payment schemes for more security. In addition smart-cards are used as official ID documents for example in Belgium together with an electronic signing function for the citizen. They are also used increasingly in the e-health sector in various European countries (e.g. Austria, Germany etc.). Official ID documents using smart card technology will be introduced in D3.6 "Study on ID Documents"¹.

3.2.1.4 Biometrics

Biometrics is essentially any kind of physical or behavioural feature a person has which can be used for verification. This topic will be described in depth in Chapter 5 with respect to forensic aspects. However, the topic of biometrics is also introduced and discussed in FIDIS Deliverable 3.2 "A study on PKI and Biometrics"².

Biometrics is becoming more widely used, for example, fingerprints will be included in the new biometric passport as defined in the ICAO³-standard for Machine Readable Travel Documents. Fingerprints have also provided a low cost solution for access to computer systems. In old military systems, retina scanners were used as secure access. Normally, the patterns of the retina remain stable over a lifetime, but they can however be affected by disease⁴. Retina scanners are not manufactured anymore. Iris scanners are used in some airports for identification of passengers crossing borders and are patented⁵. Face recognition is

¹ FIDIS Deliverable 3.6: 'Study on ID Documents', planned for March 2006

² FIDIS Deliverable 3.2: 'A study on PKI and biometrics', July 2005, available at <http://www.fidis.net>

³ <http://www.icao.org/mrtd>

⁴ <http://www.house.gov/transportation/aviation/05-19-04/05-19-04memo.html>

⁵ US5291560

the easiest biometric data to record from a person (and importantly is non invasive). More commonly, analogue photos are utilised on traditional paper based documents.

3.2.1.5 Mobile networks

The GSM (Global System Mobile) is the most widely used standard for mobile communication. When applying for a subscription on a mobile phone network, the identity of the person is often checked with bank account information and passport or other identity documents. Since someone has to pay the bills for the subscription from a bank account, in case of identity theft this will be resolved after a few months, as long as the person owning the bank account reports it. With pre-paid cards there is often no check, so this is less secure as a means to check the identity. GSM-devices are also convenient for tracking, since the geographically specific antenna data (i.e. what transponder(s) the device is near) is accessible by the service provider. The GSM's are known for their unintended audit trail. Also see Chapter 4.

3.2.1.6 RFID

The tokens for RFIDs (Radio Frequency Identification) are widely used for access to buildings. In the near future products in shops will have them available to track the product and used as a bar code. Currently RFID cards are also popular in transportation and access control (for example car rental on the street, payments for public transportation and other products, access to buildings). RFID will be technically introduced in FIDIS D3.7 "RFID"⁶ and discussed in following deliverables D7.6/7.7⁷ within the FIDIS Network of Excellence.

3.2.1.7 Digital signatures

PKI-infrastructures (Public Key Infrastructures) are used for secure exchange of digital information. PKI-infrastructure is discussed in depth in FIDIS Deliverable 3.2 "A study on PKI and Biometrics"⁸. One common open source implementation which utilises private and public keys, is called PGP⁹ (acronym for Pretty Good Privacy). Using the public key, a unique hash code can be calculated for a document allowing a person to give a 'digital signature' to the digital document. This can be used to prove that the document was not changed since it was signed. However, anyone can create a fake PGP key with your email address, just as they can lie about who the creator of a document was. What makes the PGP signature useful is that PGP public keys hook into a web of trust, so you can decide how much you trust what a person with a certain key asserts.

3.2.1.8 Conventional passwords

Conventional passwords and pin codes are often used together with a user name to gain access to a service. People tend to use the same code everywhere for their own convenience which can have security implications if the code is leaked. Notably, it is easy to copy the code if, for example, someone watches you entering the password at a keyboard.

⁶ FIDIS Deliverable 3.7: 'RFID', information will be available at <http://www.fidis.net> by September 2006

⁷ FIDIS Deliverable 7.6: 'Workshop on AmI, Profiling and RFID' and Deliverable 7.7 'Report on AmI, Profiling and RFID'; information will be available at <http://www.fidis.net> by January and August 2006

⁸ FIDIS Deliverable 3.2: 'A study on PKI and biometrics', July 2005, available at <http://www.fidis.net>

⁹ PGP www.pgp.com

3.2.1.9 Other artefacts

Many other artefacts exist, a classic example is a key for opening a door. Notably, depending on the technology that the artefact uses, they are often easy to copy.

3.2.2 Threat level

To assess the threat level for copying or modifying a certain artefact, and the risk, it is important to look what the consequences are. Points that should be considered are:

- *Is the threat now/soon/some times in the future?*

Some methods for circumventing the security system are easy to exchange over the Internet. For example if an easy method for copying fingerprints becomes available, and it is spread wide over the internet, then it will soon be used.

- *What levels of skills / resources are required? (deliberate attack)*

Threats exist which involve a lot of time to undertake, e.g. modifying the system electronics. Examples are chip cards, where people have to understand the workings of the system. However, if someone develops easy to use software allowing a person without special knowledge to copy the chip card, then clearly less effort is needed to defeat the system.

- *Ease of occurrence (accidental occurrence)*

Badly protected systems can have threats which occur accidentally. For example, in a restaurant if you pay with a credit card and they return a different credit card without you noticing, then the next time you might accidentally pay with someone else's credit card.

- *Impact*

The impact that a person using someone else's artefact has depends very much on the application. For example, access to a nuclear reactor should clearly have higher protection compared to access to a library because of the potential impact such a breach may ultimately have.

3.2.3 Forms of failure

There are several reasons as to why a system may fail. Described below are some of the most common.

3.2.3.1 Central system misled

If a person has access to a central system, for example the administrator of a banking system, then they often control the whole system, making fraudulent bank transfers possible. Since the central system is based on trust and often fast action is necessary, this is one of the most difficult attacks to prevent.

3.2.3.2 Wrong person identified / misidentified

Another possibility is that the wrong person is identified. This can happen for example if two persons have the same passwords and user name, or when two people have the same name and date of birth. This can either be deliberate or accidental.

3.2.3.3 Incorrect information about individual propagated

Once the wrong information is entered in a system, it may be copied to other systems. For example, if a bank makes a spelling error in a name when entering it in the system, the same information could be used for credit cards and other systems or devices that are used. This is unless there is a connection to a central database with the official data and software that checks for this type of error.

3.2.3.4 Leakage of information to unauthorised persons

With the expanded use of credit card databases and online shops, the risk of sensitive information leakage to unauthorised persons increases. An example of this is a case in California, USA where 40 million¹⁰ credit card numbers were leaked out of the systems of data brokers. However, this is not limited to credit card data; any information can potentially be leaked from source by a variety of methods, such as medical data from hospitals.

3.2.3.5 Poor issuing procedures

Often management during the issuing procedures has an important impact on the failure rate. This is because security can be viewed analogously as a chain, where the weakest link in the chain will be the one most likely to break. If the issuing procedures around ID documents are not sufficient, then the complete security-chain may have the wrong identity for a person. For example, if the bureau that handles ID-card requests does not verify the information of the person requesting a new passport, it is possible that, according to the documents, two different persons have the same identity but with different pictures on the passports.

3.2.3.6 Ease of cloning

If an artefact is easy to clone, then it is likely to be exploited, as can be seen in recent ATM-fraud cases¹¹. Here, a relatively simple method allowed people to copy magnetic stripes and PIN codes by using manipulated ATMs, which were subsequently used to fraudulently remove money from the victim's bank accounts.

3.2.3.7 Ease of data alteration

In some cases data alteration is very easy. Some on line banking systems make it easy to change addresses of a person, without the owner of the credit card being aware that the address has been changed¹².

3.2.3.8 Compromise of communications channel

It is well known that unencrypted data is easy to read if someone has access to the communication channels or networking devices in between. Examples are weakly encrypted wireless networks where someone sends sensitive information. These are becoming increasingly common in internet applications.

¹⁰ http://tb.news.com/tb.cgi/2100-1029_3-5751886

¹¹ http://www.atmmarketplace.com/news_story_13115.htm

¹² http://finance.yahoo.com/creditreports/creditreports/privacy_and_fraud/article/101273/The_Credit_Industry_is_Taking_Measures_to_Combat_Credit_Fraud

3.2.3.9 Technical, management and human failures

In some cases the management gives permission to the employees to modify data and add or delete records. This will give an extra risk for failure of the system if misused by the employee. Also people might give out passwords or other sensitive information to the wrong person on the phone for example (well known social engineering attacks of systems¹³). In addition technical reasons can result in unpredictable behaviour of systems. This might occur in a central database where a worm or virus is changing the data.

3.2.4 Verification problems

With the verification (one to one comparison) of a person, there can be problems that occur due to the procedure or the system that is used. For example, if the false rejection rate of the system is high due to the algorithms used, a person that should have access is denied access. Of much higher consequences are high false acceptance rates. In this case a user that is not a valid user is authenticated by the system (and subsequently given access). Biometrics is especially vulnerable to these kinds of problems (see for example FIDIS Deliverable D3.2¹⁴).

3.2.4.1 Reading accuracy

How accurately does the system read the information? An aspect is the manipulation of sensors. For example it is possible to damage a fingerprint sensor by using a strong acid fluid, without anyone noticing it. Especially when enrolling new users using a manipulated sensor as described above, this can have severe consequences for the authentication process performed subsequently, especially when enrolling new users using such a manipulated sensor later.

3.2.4.2 Local / central verification

Often an iris is compared with the IrisCode¹⁵ stored for example in a chip card. Once it is known how to alter the information in the chip card, it is possible to store a different IrisCode instead of the one originally entered in the system. If a central verification system is used for storing biometric templates and manipulation occurs, the reliability of the entire system is affected.

3.2.4.3 Speed of response

If an authentication system for example at a border works too slowly, then a risk exists that the operators of the system will simply skip the check to prevent queues.

3.2.4.4 Reliability of communication facilities

It is possible for the communication facilities to be attacked such that the system cannot communicate any more, for example to perform verification against a central database. To prevent this, manual or technical backup procedures have to be in place.

¹³ <http://www.securityfocus.com/infocus/1527>

¹⁴ FIDIS Deliverable 3.2: 'A study on PKI and biometrics', July 2005, available at <http://www.fidis.net>

¹⁵ <http://www.cl.cam.ac.uk/users/jgd1000/binomdata.html>

3.2.4.5 Confidentiality of process

How confidential is the process overall? If for example fingerprints are communicated without encryption or with weak encryption then unauthorised people might intercept the fingerprint data from the database and produce a fake copy.

3.2.4.6 Authentication of enquirer

Is the person enquiring information really the person that should receive the information? Authentication of the operators of the system is an essential issue.

3.2.4.7 Costs of infrastructure

In any kind of implementation the costs are important for the manufacturer. For instance, a fitness club will not invest in expensive biometric equipment and in these cases often cheap sensors and systems are used where the fingerprint data is not stored in a secure way. As such, a high risk exists that the data will be stolen, especially if the system is connected to the internet with insufficient protection.

3.2.5 Consequences of failure**3.2.5.1 Identity theft**

One of the best known consequences of failure is identity theft. This might cause financial loss, for example, because the wrong person is given a loan or could. Identity theft is further examined in deliverable D5.2¹⁶.

3.2.5.2 Legitimate person wrongly accused

One of the possible consequences of identity theft is that the wrong person may be accused of a crime. In these cases it is well known that people can lose rights for obtaining jobs, or access to their money.

3.2.5.3 Wrong information associated with individuals

It has been seen in documented cases¹⁶ that the association of incorrect information with an individual can have immense ramifications. Two examples are given below.

- **Wrong medical treatment**

In cases where medical history records have been misused by someone for insurance reasons, it is possible that in an emergency the wrong data are in the database (i.e. the data of someone who used the victim's insurance contract). This might cause the situation whereby the wrong medical treatment is given.

- **Wrong credits granted**

Other cases of identity theft can result in, for example, denial of boarding at an airport due to information that is not correct in the database. Another example is refusal of mortgages since loans have been given to someone else without the victim knowing it.

¹⁶ FIDIS Deliverable 5.2: 'Workshop on Identity Fraud and Identity Theft', report available at <http://www.fidis.net>

3.2.5.4 Loss of confidentiality

If a certain password or biometric property is frequently used for different services, then if the information is leaked, it can be used to gain access to all of the services that use it. For example, credit card companies often use questions concerning date of birth or the maiden name of the mother for authentication purposes on the phone. Since this same information is often used by a variety of service providers and is thus stored in many databases around the world, if just one database gets stolen then it becomes easy for a criminal to answer these security questions to another company that uses the same data.

3.2.6 Forensic aspects

For forensic science, it is important to know the reliability of the identity management system, and that the evidence extracted from the system can be explained in court. We distinguish the following issues:

3.2.6.1 Reliability of underlying technology

How good is the technology, and is it easy to alter the data that identifies a certain person? In forensic science it is important to understand the underlying technology that is used. In the old-fashioned passport the question is, for example: how easily can someone change the photograph in the passport?

3.2.6.2 How well is individual bound to ID artefact?

It is often quite easy the exchange paper passports. In the case of look-a-like fraud, another person can use a passport at the border without anyone realising it. Furthermore, in some countries it is relatively simple to switch identity, by asking the government for a change of names.

3.2.6.3 Auditability

Can we audit the complete system and determine how it works, for example a card system? Do we have log records of for example a payment system?

3.2.6.4 Transparency

A question that arises is whether the forensic scientist actually has access to the artefact data and technology. If not, they might look at it as a 'black box', but the essential issue is the validation of the information extracted from the system. In many cases trade secrets are a hindering factor. Open source projects in general give more insight in the technology that is used.

3.2.6.5 Disclosure

With many proprietary systems it is not known if there are 'back doors' in the software, which allow the manufacturer (and thus anyone else that becomes aware of it) to circumvent the protection system. However, not everything can be disclosed in a court room, since manufacturers also sometimes have non-disclosure agreements with the expert. The reason is that they do not want to share methods with the public, or that the government would not like to disclose a certain method, since then it will not be useful in future cases.

3.2.6.6 How long is data kept?

To examine data, it is important to know how long the data is kept. Surveillance systems are known to typically keep their data for several days, after which they will overwrite it. These kinds of issues have to be taken into consideration. In some cases additional information can be extracted from data caching or other areas where the information was temporarily stored.

3.2.6.7 Ethical issues

A forensic scientist should also know the rules relating to data protection legislation. Often in criminal law the system can be examined. However, whether it is admissible in court depends on the laws of the country and how the information was gathered. For example, in the Netherlands wiretaps are commonly used as evidence in court, whereas in the United Kingdom this is not admissible, which is based on the ethics within a law system. Other ethical issues one should be aware of are, for example, that personal details may become available from the data that is extracted.

3.2.6.8 Unintended audit trail

Unintended aspects are aspects of the artefact or the means of using it which yield information of forensic value. In some cases useful information such as GSM location data can be extracted. Using this data for locating someone goes beyond the original purpose of the network provider storing this information, which was for billing purposes.

3.3 Conclusion

Using this model as a basic framework, as an exemplary case study we shall examine mobile phone networks for their ability to provide reliable identifying information in the forensic context. Further, the use of biometrics as a unique identifier will be considered.

4 Case study: Reliability of Identification in Mobile Phone Networks

4.1 Introduction

Today mobile communication has become a matter of course for many people. Indeed, domain experts expect mobile communication networks to take over the role of fixed-line networks in voice communication in the near future¹⁷. In this context subscriber identification is not only important to Mobile Network Operators (MNO) but also to third parties such as providers of value-added services or forensic investigators requiring reliable identification of initiators or network activities. Since mobile communication standards as defined by the network operator conglomerate Groupe Spécial Mobile (GSM) for instance have reached global acceptance, the service subscriber's mobile phone number – technically termed Mobile Subscriber Integrated Services Digital Networknumber (MSISDN) – has become an interoperable ID artefact.

The reliability of identification in mobile communication networks is important from two perspectives: First there is commercial interest of the MNO in undeniable billing of provided services. Since the introduction of non-voice value-added services – such as Premium Short Message Service (SMS) services and download offers – this interest has expanded to third parties that rely on the transmitted MSISDN for charging of their services. The second perspective on MNO data is of a forensic nature: Since the number of subscriptions to mobile communication services exceeds the number of inhabitants in some European countries, most persons are likely to carry a mobile communication device with them and records of time and location of subscriber activities may thus provide valuable information for forensic examinations.

4.2 Applying the forensics model

The following paragraphs will examine the reliability of identification in mobile communication networks using the forensics model as derived in section 3 as the framework for analysis.

4.2.1 Threat levels

The results of forensic examinations can only be as reliable as the information based on which they were carried out. Depending on whether the reliability of identification is threatened by faulty or missing subscriber data or technical manipulations, threats to reliability of identification information can be categorised into those arising at account or technical level. Figure 4-1 visualises important entities in this context: A subscriber (in GSM networks technically represented by the Subscriber Identification Module (SIM) card) communicates with the network which in turn creates Call Detail Records (CDRs) to document service provision. These records are stored and processed by the billing system that links the identification number of the SIM – the International Mobile Subscriber Identity (IMSI) – to a subscriber account. The following paragraph describes the risk of misidentifications at this level.

¹⁷ Exane BNP Paribas: Mobile Operators – More Effort required. Paris, January 2005



Figure 4-1: Schematic overview between mobile, network and billing

4.2.2 Threats at Account Level

One has to be aware of the very different motivations of MNOs and forensic experts. With respect to subscriber identification: While the former focus on the reliable assignment of billing records to accounts, forensic experts are interested in assigning actions to persons. Differences between both approaches become obvious with respect to prepaid contracts: Since there is no risk of non-payment, subscriber identification is of little interest to the MNO (except for marketing campaigns). As such, MNOs usually only ask for proof of identity for prepaid contracts if required by law and often the collected data is of poor quality. Often registered SIM cards are sold on flea markets or internet auction sites making it easy to obtain access to mobile communication services under another (the registered) person's identity.

Different from prepaid contracts, post-paid contracts create bad debt exposure to MNOs. Consequently post-paid contract applications are subject to careful screening of ID documents for attempts of fraud. These measures turn the setup of a post-paid account on another person's name – so called Subscription Fraud – into a difficult task. In addition the fraud – if not accompanied by the fraudulent setup of a bank account – will be discovered soon after the first billing cycle since the assumed account holder will deny payment and report the fraud to the customer service of the MNO. In the meantime the fraudster may have raised important bills – however from a forensic perspective checks of ID and subscription application documents will likely allow to clear the “account holder” from wrongful allegations.

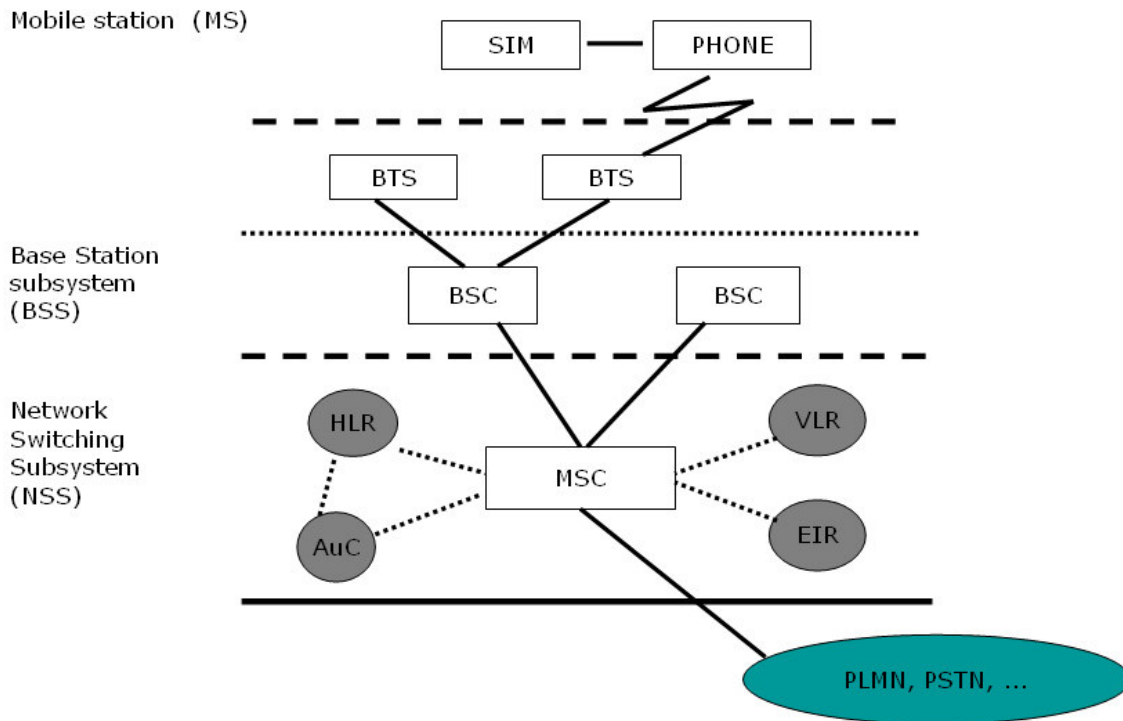


Figure 4-2: Standard architecture of a GSM network

4.2.3 Threats at a Technical Level

The discrimination between account holder and actual user of a service becomes difficult or impossible if manipulations are carried out on a technical level to deceive the network about the actual subscriber ID. These kinds of manipulations may happen at the interface between the network and the mobile station (that is between Mobile station (MS) and BTS in Figure 4-2) or at gateways to other Public Land Mobile Network (PLMN) and fixed-line Public Switched Telephone Networks (PSTN). First we will investigate ways to manipulate the identification at the air-interface.

Manipulation of the IMSI

In GSM networks a subscriber is identified by the IMSI stored on a PIN-protected SIM card. The IMSI is a usually fifteen digit number composed of a three digit country code, a two or three digits network code and a unique subscriber number. The IMSI is used as a lookup key with the Home Location Register (HLR) to verify a subscriber’s authorization to access the network.

Manipulations of the IMSI – allowing an attacker to use another person’s network identity – became possible due to vulnerabilities of the authentication algorithms COMP128 used for authentication of the Mobile Station (MS) to the GSM network. The authentication process is visualized in figure 4-3 and includes the following steps: (1) In order to register with the network the MS sends a registration request to the Mobile Switching Center (MSC). (2) The MSC forwards the MS’s IMSI to the HLR and request a data triplet for authentication of the

MS. This triplet includes the key *kc* for encryption of the communication between MSC and MS, a random number *RAND* and the secret response *SRES* calculated by the COMP128 algorithm based on *RAND* and the subscriber’s secret key *ki*. (3) Upon request by the HLR the triplet is generated by the Authentication Center (AuC) and forwarded to the MSC. (4) The MSC communicates *RAND* to the MS and requests it to calculate *SRES* based on the *ki* stored on the SIM. If responded *SRES* (5) matches the *SRES* previously calculated by the AuC (6) the secret keys *ki* on the SIM and at the AuC match and the subscriber is authenticated. For a detailed description of the process see reference¹⁸.

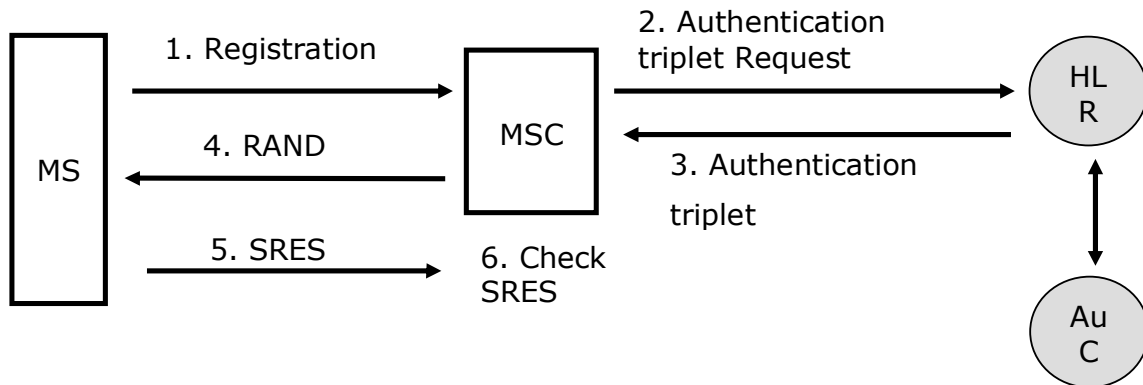


Figure 4-3: Authentication Process of Mobile Station to the Network using COMP128

Researchers at UC Berkeley to whom the COMP128 code was leaked in 1998^{18 19}, managed to deduce the SIM’s secret key *ki* from COMP128 responses to random numbers. Network operators that had implemented the GSM *Memorandum of Understanding’s* algorithm without modifications were proved to be vulnerable to *ki* extraction attacks. The researchers also found that the voice privacy encryption key *kc* was zeroed on 10 bits. The understanding of COMP128 – sometimes referred as COMP128 v1 since revised algorithms became available – and the shortened *kc* key allow creating copies of a SIM: This process is known as SIM Cloning.

To encounter SIM cloning network operators have introduced *Velocity Checks* that verify the plausibility of location updates communicated to the HLR: If a SIM and its clone register from different cells, an alarm will be raised and one of the cards be logged out. An important condition for SIM cloning is physical access to the SIM and the knowledge of its PIN – a theoretically possible over-the-air attack has never been realized in practice. These restrictions make it easier to identify SIM cloning fraudsters such as dishonest dealers that create SIM clones prior to handing SIM and PIN over to customers. As a result SIM cloning has never become an important economic threat to GSM network operators. Still, in order to assure customer confidence many operators have decided to upgrade their authentication algorithms.

¹⁸ Weis, R., S. Lucks: Sicherheitsprobleme bei Authentifizierung und Verschlüsselung in GSM-Netzen. Datenschutz und Datensicherheit, 22 (1998), pp. 504-508

¹⁹ Anonymous, GSM-cell phones cloned, website online at: <http://jya.com/gsm-cloned.htm> [Accessed 15-09-2005]

As third generation mobile phone communication standards (3G) such as the Universal Mobile Telecommunication System (UMTS) are implemented, one can expect the importance of SIM cloning to diminish since a number of improvements have been taken^{20 21}. In particular the implementation of two-side identification – where the network has to identify to the SIM in order to request authentication – will put important restrictions on cloning the SIM. An issue may however arise from the stretched migration of GSM subscribers to UMTS that requires the UMTS SIMs to be compatible with older and less secure GSM algorithms.

Manipulations of the sender ID transmitted to the network

Besides SIM cloning an attacker could deceive forensic analysts about subscriber activities by calling or sending an SMS to a subscriber from a PLMN or PSTN using a manipulated sender ID. To the author's knowledge the manipulation of a fixed line phone number requires physical access to the network infrastructure, a call from a manipulated mobile phone requires a cloned SIM as described above. A more easily implementable deception is SMS sending through a commercial gateway that allows sender ID specification. In this case, the sender ID can only be verified by checking the assumed home network for corresponding billing records. A fraudulent business case may result from subscribing third parties to premium services through faked subscription SMS. However in most environments foreign SMS gateways cannot route messages to only network internally used short code registration numbers. As a result the fraud scheme of faked subscription messages is not realisable.

To summarise: The reliability of identification by mobile communication networks is threatened on different levels: First, the mapping of an IMSI to a person might be faulty if application data have not been verified or if the SIM has changed owner without registration update (as it is often the case for prepaid subscriptions). Second, there exist ways to manipulate the IMSI itself: With respect to SIM Cloning there is thus no absolute certainness about the subscriber's identity. Important restrictions – such as physical access to the SIM and knowledge of the PIN, revised (and unpublished) authentication algorithms, velocity checks of HLR updates and detection of double registrations as well as limited numbers of authentication runs – turn its practice however in a low risk. This is different for SMS spoofing: The ease of faking the sender ID and in addition the necessity of extended search in billing or SMS centre databases to prove the spoof may turn this manipulation scheme into a fraudsters' favourite.

4.2.4 Forensic reliability

To investigate the forensic reliability of network data one should start from the list of involved entities: Usage records are collected into databases as a subscriber requests (or receives) services from the network. In this context the corresponding account is identified by the IMSI, complementary the network device's serial number, the International Mobile Equipment Identity (IMEI) is submitted.

First we investigate the assumed bounding of the SIM to a person: The card – and therefore the network ID – is transferable. As stated in section 4.2.2, registered prepaid SIM cards are

²⁰ Pütz, S., R. Schmitz, T. Martin: Security Mechanisms in UMTS. Datenschutz und Datensicherheit, 25 (2001) X, pp. 1-9

²¹ Martin, T., S. Pütz: On the Security of the UMTS System. Proceedings of "GI-Fachtagung VIS'2001". DuD-Fachbeiträge, Vieweg, Braunschweig, Wiesbaden, 2001, pp. 87-106

often sold at flea markets – as a result the bounding of a SIM to a person is only indirect evidence that actions were carried out by the account holder. Such a bounding is often assumed in interceptions – and often has to be verified by voice comparison, that does not however provide very strong evidence of a person's identity. As a result, the reliability of the assignment of a SIM to a person in many cases is not very strong and may be disvalued by a – probably only claimed – theft of the handset.

The second bounding to approve is the assignment of an IMSI to a particular SIM. As described in section 4.2.3, SIM cloning allows programming of a SIM so that it carries a different IMSI. As a result, records may not reflect the activities of the original SIM but its clone. This is an important threat to the overall forensic reliability of MNO records – it however has only little practical impact since cloning is very, very seldom carried out in practice.

A third option available to investigators is the serial number of the handset used: Similar to the SIM, the handset can be shared between persons. The IMEI can also easily be reprogrammed and different handsets may carry the same serial number as a result. The IMEI information is also not available from all networks: Particularly for roamers MNOs often do not deliver the IMEI information to the home network. Essentially, this means that the IMEI only provides weak evidence of the user's identity.

The forensic reliability of collected data also depends upon the software used to store and process it: To assure data is not altered upon access to the SIM or the phone the software should be audited. In theory this is also true for the MNO's billing system that stores the network signalling data in databases. Eventual failures may lead to unreliable data – this aspect is highlighted in the following paragraph.

4.2.5 Forms of failure

In general, failures of mobile network identification lead to non- or misidentification of subscribers. In the first case the initiator of certain network activities cannot be named while in the second the wrong subscriber is identified. The causes for such failures may result from the external or internal manipulation of entities, failure in the service delivery and the data collection process. While the previous paragraphs have outlined means of third parties to undermine the reliability of identification, we now look at internal causes that may lead to identification failures. Such issues may occur at a technical or a management level and result in inconsistent data flow between network entities or inaccurate information in the billing databases.

The most important technical issues are related to incomplete data feed of the MSC to the billing system. In this case not all subscriber activities have been communicated to the billing system and thus information provided to investigators is incomplete. Obviously this is a major risk to MNO business operations and many companies employ revenue assurance teams to steadily verify the accuracy and completeness of billing records.

If a subscriber roams with a foreign network data quality is only controlled by the visited network. As these get paid for service provision based on transferred billing records, operators are motivated to deliver complete data and in result subscriber activities abroad are still transparent – after a certain time lag – to the home network and investigators.

Issues of misleading information of subscriber activities may also result from data being altered when being archived. We assume that this risk mainly exists at the interface between MSC and billing system as a network internal corruption of signalling data would have caused

the entire service request to fail – and no billing event would have been raised anyway. The data alteration may result in wrongful (or failing) linkage of service usage to a subscriber account. As such a malfunction would result in large-scale billing errors it would likely be detected and corrected quickly – we therefore regard the risk of consistent malfunctions as small.

On a management level the reliability of collected data may be undermined by fraudulent employees or contractors. Even if systems have been set up as tamper-proof against manipulations from outsiders, internal fraudsters – for instance system administrators – may still bypass security measures. The related risk grows by the number of people that have access to systems. In this context the complex, heterogeneous Information Technology (IT) landscape of telecommunication companies may very well be vulnerable. However besides manual data manipulation, the risk of information leakage – for instance about interception activities – may still be of more importance to investigators. A well-known example was reported from a German MNO who – after a software update – accidentally billed interception call forwards to subscribers, who that way learned about the investigations under course.

4.2.6 Consequences of failure

Independent from the actual causes (MNO internal or external), identification failures lead to the loss of identity of the legitimate subscriber: Actions taken by a third person to a subscriber's account may well lead him to be confronted with wrongful allegations. The actual damage of the Identity Theft depends on how quickly the illegitimate use of the subscriber ID is detected and what the costs of re-establishing the original status-quo are. In this context one may distinguish 'direct costs' – resulting from unlawful service use on the subscriber's account and replacement costs for SIM card and mobile phone – and 'indirect costs' of efforts to prove one's innocence. A subscriber may also suffer from loss of confidentiality if personal information were retrieved from the SIM or handset. From a technical point of view a new IMSI – then linked to the original MSISDN – can be issued by the MNO without problems. The major hassle – as with all types of identity theft – lays in broader issues of clearing credit reports or restoring suspended service deliveries.

To conclude, the main concerns regarding failures of identification based on mobile phone network ID artefacts are non-financial: Since mobile phone service providers report non-payment or fraud to credit bureaus the abuse of one's identity in the telecommunication domain may have negative implications for business relationships with other organisations too. Clearing one from wrongful associations of information from non-obvious fraudulent abuse of one's identity may turn out still more difficult: Take as an example the efforts required to prove that movements between network cells registered by the phone network operator have been results of activities of a third party using a cloned SIM.

4.3 Conclusion

This paragraph summarises our findings on the reliability of identification in mobile phone networks. In reference to the forensic aspects outlined in chapter 3, we found that the reliability of underlying technology differs for the services used: While SMS sender IDs can easily be spoofed, the cloning of a SIM card in order to use voice or data communication on another subscriber's account is much more difficult and even impossible if corresponding vulnerabilities of the technical infrastructure have been fixed by the network operator. Verifying with the operator which version of COMP128 is used should allow quantifying the risk of SIM cloning in a particular case.

The bounding of the ID artefact to an individual is judged as weak: This is particularly true for pre-paid contract schemes where MNOs have no personal interest in the verification of subscriber identities. Subscriber data provided for forensic investigations therefore require careful investigations with regard to reliability. For post-paid contract schemes the number of invoices paid to date will help to judge the risk of subscription fraud: Fraudulent accounts usually feature no paid invoices.

The criteria of audibility, transparency and disclosure cannot be answered in regard to the general character of this document: Signalling and billing data processing is usually customized to operator IT requirements and access therefore subject to individual policies.

The length of data storing and concerns of ethical issues in using the data depend on local legislations. From a billing perspective data is usually only required for a maximum of six weeks (that's the usually monthly billing cycle plus two weeks for data processing), longer storing is usually only due to legal requirements.

5 Case Study: Biometric Artefacts

5.1 Introduction

Providing certain conditions are met, biometric artefacts can be used to achieve reliable, fast and secure verification of the identity of a user that is attempting to access a system. Such access includes logical access to information systems, such as computers or networks, or physical access to facilities such as buildings or across borders. However, here we shall examine how reliable current systems are, and as such how useful they are in the forensic context.

The International Biometrics Group (IBG) uses the following technical definition²² of biometrics:

‘The automated measurement of behavioural or physiological characteristics of a human being to determine or authenticate their identity’

For a more extensive introduction to biometrics and a treatment of various aspects of biometrics and identity outside of the scope of this document, the reader is referred to FIDIS Deliverable 3.2²³.

Successful deployment of biometric access control systems can, apart from increasing system security, tie persons to events, such as a user accessing a system at a certain time and/or location. Such traces can be helpful in forensics, for instance for determining potential system trespasser identities or verifying alibis.

One of the conditions for successful deployment is that the biometric authentication system is presented with genuine biometric samples. This chapter shows that typical biometric devices cannot at this point discern whether or not this condition is met. Tests were done that involve manufacturing forgeries of fingerprints, irises, hands and vascular patterns and using those to circumvent the intended functionality of biometric device technologies. The tests demonstrate that the security offered by biometric systems is not failsafe, consequently diminishing the forensic reliability of user traces in such systems.

It must be stressed that the tests are at this point qualitative in nature, purely demonstrating the practical possibilities of fooling the devices. The tests do not provide enough data to conclude that any biometric template can be approximated by presenting the devices with fake biometric samples.

Section 5.2 gives a concise overview of biometric artefacts and the technological principles that the biometric devices tested are based on. In section 5.3 a general overview is given of potential forms of failure of biometric systems, to allow the specifically investigated threat areas to be placed in context. Section 5.4 introduces the specific biometric device models that were tested. For the fingerprint scanners, an overview is shown of the influence that scanner technology and varying skin conditions have on device output, which in turn influences verification quality. Section 5.5 deals with the threat level of artificial biometric artefacts by showing how and to what extent the devices could be fooled by these. In the final section, conclusions are drawn, addressing consequences of failure and the forensic aspects of biometric access control systems.

²² International Biometrics Group website, <http://www.biometricgroup.com/US-VISIT.html>

²³ ‘FIDIS Deliverable 3.2: A study on PKI and biometrics’, July 2005, available at <http://www.fidis.net>

5.2 Biometric artefacts used for identification and verification

5.2.1 Overview

Table 5-1 lists biometric artefacts that have received attention in the research and development industry because of their potential for automatic identification and verification of persons. Not all of the biometric features from this table have yet yielded commercial applications, gained a foothold in the market, or indeed show promise of doing so in the near future.

Physical characteristic:		
Biodynamic signature	Finger geometry	Nail
Bioelectric field	Finger surface (3D)	Odour
Bite marks	Finger wrinkles	Palm print
Bone sound transmission	Fingerprint	Pores
Cardiac pulse	Hand geometry	Reflection of acoustic waves in the head
Corneal surface topography	Hand pressure profile	Retinal pattern
Dental geometry	Hand thermogram	Skin impedance
DNA	Hand vein pattern	Skin pattern
Ear	Iris	Skin spectrum
Facial geometry (2D / 3D)	Knuckle creases	Smile
Facial thermogram	Lips	Voice print
Behavioural characteristic:		
Dynamic grip recognition	Handwriting	Tapping
Eye movement tracking	Keystroke dynamics	
Gait	Mouse dynamics	

Table 5-1: List of biometric artefacts having received attention because of their potential for automatic recognition of persons^{24 25}

²⁴ Mainguet, J.F., Page d'accueil du site de Jean-François Mainguet, available at <http://perso.wanadoo.fr/fingerchip/>

²⁵ Maltoni, D., Maio, D., Jain, A.K., and Prabhaker, S., Handbook of Fingerprint Recognition, Springer-Verlag, New York, June 2003

For this document, we have focussed on the physical characteristics that are currently most commonly used as biometric identifiers in biometric devices, as well as some that show promise. Notably, facial geometry (2D and 3D) shows great promise, although this is not in the scope of this document. The technologies used in biometric devices that involve the selected artefacts are explained next. For the remaining artefacts mentioned in Table 5-1, the reader is recommended to follow up on the Mainguet website²⁶, which is an excellent starting point for further information.

5.2.2 Fingerprint

Fingerprint recognition using biometric devices involves taking fingerprint images from fingertips. Patterns of fingerprint ridges and valleys are detected and stored in a simplified data format (a small file called a user ‘template’) which can be used for comparison with other fingerprint templates for verification or identification. The images are acquired with some kind of sensor. A variety of fingerprint sensor technologies are used in commercial fingerprint scanners^{27, 28}:

Optical sensors:

- *Frustrated Total Internal Reflection (FTIR)*

This technology is based on the behaviour of light at boundaries from one material to another. The finger is placed on the top side of a glass prism (see Figure 5-1). Light entering the prism from a Light Emitting Diode (LED) on one side of the prism is partially reflected at the contact surface and then captured via a lens with a light-sensitive chip (for instance Charge Coupled Device (CCD) or Complementary Metal Oxide Semiconductor (CMOS) image sensors) on the other side of the prism. Image contrast is caused by the fact that light is randomly scattered or absorbed at the points where skin ridges and the prism make contact, and totally reflected at the valleys, where no contact is made.

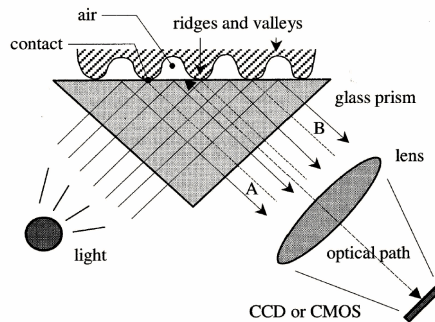


Figure 5-1: An FTIR-based fingerprint sensor²⁷

²⁶ Mainguet, J.F., Page d'accueil du site de Jean-François Mainguet, available at <http://perso.wanadoo.fr/fingerchip/>

²⁷ Maltoni, D., Maio, D., Jain, A.K., and Prabhaker, S., Handbook of Fingerprint Recognition, Springer-Verlag, New York, June 2003

²⁸ SecuGen Biometric Solutions, ‘SEIR™ Optic Technology’, available at http://www.secugen.com/download/SGWP_SEIR.pdf

– *Surface Enhanced Irregular Reflection (SEIR)*

This technology shares some characteristics with FTIR technology. The contrast between ridges and valleys is also brought about by the different behaviour of light after hitting the ridges and valleys. In this case, however, the light hits the contact surface perpendicularly (see Figure 5-2), scattering at the ridges but completely passing at the valleys so no scattering occurs. The scattered light is collected by the image sensor, thus produces bright spots for ridges and dark spots at valleys. The sensor manufacturers claim that this technology gives higher contrast images than FTIR technology²⁹.

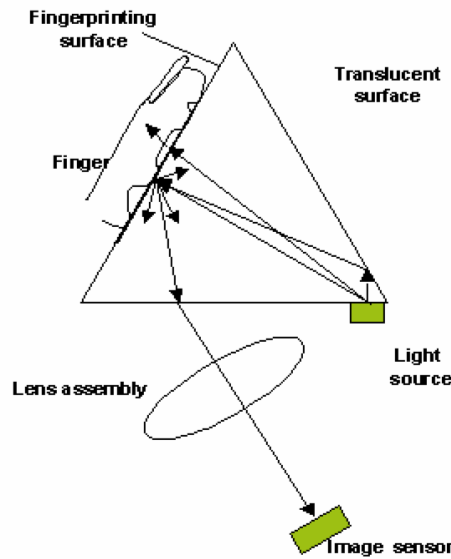


Figure 5-2: A SEIR-based fingerprint sensor²⁹

– *Electro-optical*

These sensors use a layer of light-emitting polymer, of which the light emission varies based on the potential applied on one side (see Figure 5-3). When placing a finger on the polymer surface, ridges touch the polymer and valleys do not, causing the potential to vary across the surface. Thus, a luminous representation of the fingerprint is generated. A second layer, consisting of a photodiode array or a CMOS, converts the light pattern into a digital image³⁰.

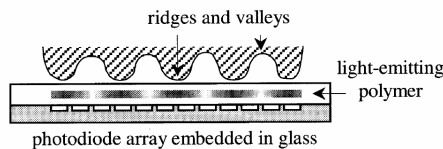


Figure 5-3: An electro-optical fingerprint sensor³⁰

²⁹ SecuGen Biometric Solutions, ‘SEIR™ Optic Technology’, available at http://www.secugen.com/download/SGWP_SEIR.pdf

³⁰ Maltoni, D., Maio, D., Jain, A.K., and Prabhaker, S., Handbook of Fingerprint Recognition, Springer-Verlag, New York, June 2003

– *Touchless*

In this case a high-quality camera is used to focus on the fingertip and directly read the fingerprint. Usually some kind of mechanical support is present to facilitate presenting the finger at a set distance.

Solid State sensors:

– *Capacitive*

A capacitive sensor is a two-dimensional array of micro-capacitor plates embedded in a chip. The finger skin acts as a second micro-capacitor plate (see Figure 5-4). Small electrical charges are created between the array and the finger, of which the magnitude depends on the distance between the surfaces. As such, the resulting capacitance pattern represents the ridge and valley pattern of the fingerprint.

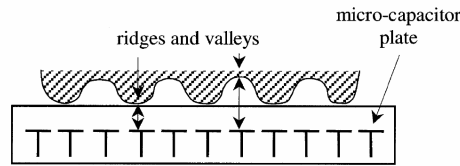


Figure 5-4: A capacitive fingerprint sensor³¹

– *Electric field*

This type of sensor generates a small radio-frequency field, which is modulated by the highly-conductive sub-surface of the skin (live skin cell layer). A matrix of antennas receives the modulated analogue small-amplitude signal, which is then further processed and digitised to obtain an image representing the contours of the live skin layer³².

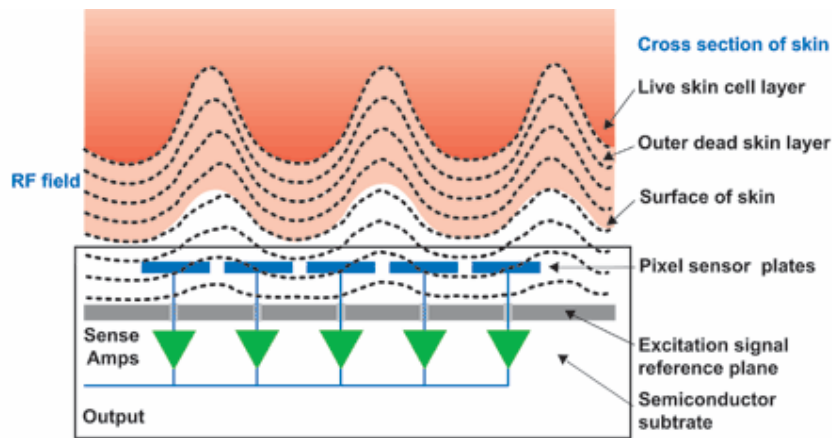


Figure 5-5: Electric-field fingerprint sensor³²

³¹ Maltoni, D., Maio, D., Jain, A.K., and Prabhaker, S., Handbook of Fingerprint Recognition, Springer-Verlag, New York, June 2003

³² Authentec, Inc. website, <http://www.authentec.com>

- *Piezoelectric*
 These sensors make use of the piezoelectric effect. The sensor surface is made of a non-conducting dielectric material which generates small amounts of current when pressed. The amount of current depends on the pressure applied. When pressing a fingertip on the sensor, the ridges will apply a higher pressure than the valleys as they are closer to the sensor surface. Typically, the sensor material uses some kind of threshold to determine whether or not a sensor element is ‘pressed’, thus only enabling acquisition of binary images³³.

- *Thermal (sweep sensor)*
 These sensors are made of pyro-electric material that generates current based on temperature differentials. Sweeping a finger across an electrically heated sensor allows measurement of heat flow to the skin, which is higher at direct contact with the sensor, thus allowing distinction between finger ridges and valleys^{33, 34}.

Other sensor types:

- *Ultrasonic*
 This type of sensing is based on sending acoustic signals towards a fingertip and capturing the echo signal. As each change of impedance gives a partial echo, this technology can be used to image the sub-surface of the skin³³ (see Figure 5-6).

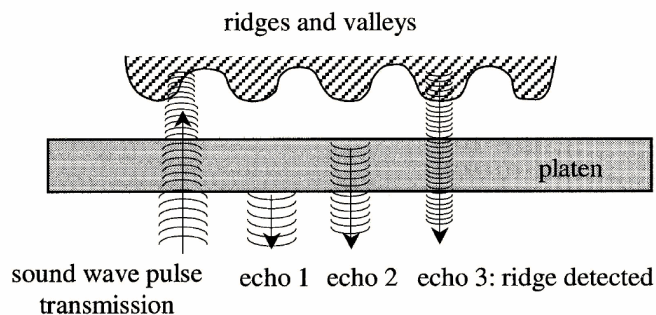


Figure 5-6 : The principle of ultrasonic sensing of a fingerprint³³

5.2.3 Iris

Iris recognition technology uses a near-infrared light source and optical camera to capture an image of the iris. Using pattern recognition algorithms, the image is converted to a template (also known as IrisCode³⁵) which allows comparison with other enrolled templates (see Figure 5-7).

³³ Maltoni, D., Maio, D., Jain, A.K., and Prabhaker, S., Handbook of Fingerprint Recognition, Springer-Verlag, New York, June 2003

³⁴ Mainguet, J.F., Page d'accueil du site de Jean-François Mainguet, available at <http://perso.wanadoo.fr/fingerchip/>

³⁵ Daugman, J., 'High confidence visual recognition of persons by a test of statistical independence.', IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 15(11), pp. 1148-1161, 1993

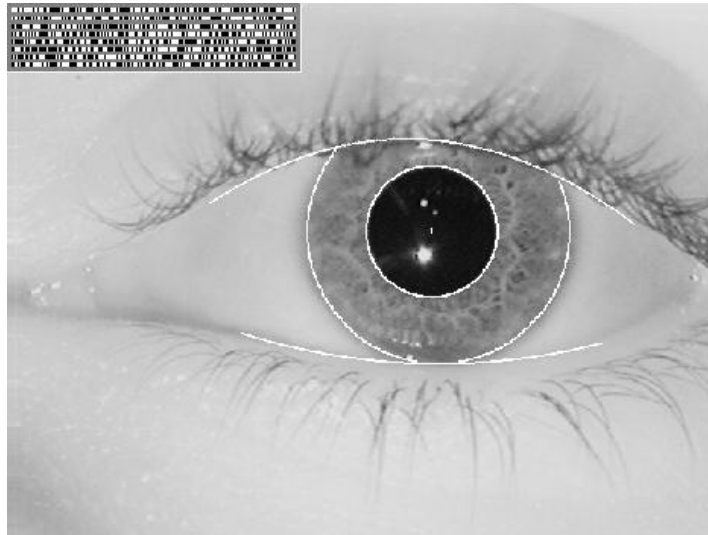


Figure 5-7: Iris pattern and IrisCode³⁶

5.2.4 Hand geometry

Hand geometry recognition is currently mainly used for physical access control applications. Typically, devices using this feature map the size and shape of a person’s hand, compute a template from it and verify this with a previously enrolled template.

A source of light illuminates two perpendicular mirrors and the reflected light is captured by the device. When a hand is inserted at the proper location (using guidance pegs) it partially blocks the light reflecting from the mirrors, thus creating a silhouette image on the sensor of both the top view and the side view of the hand (see Figure 5-8).

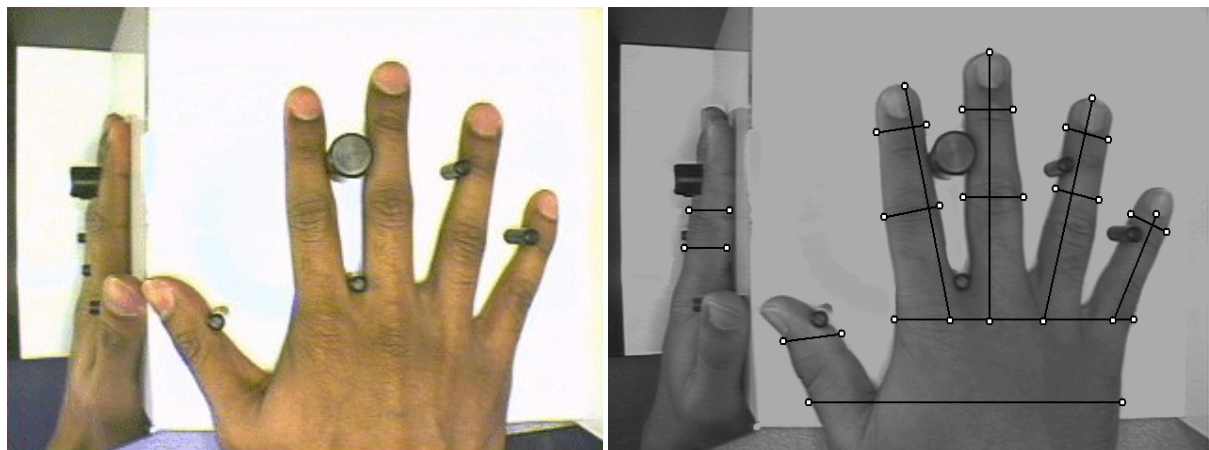


Figure 5-8: Hand geometry recognition³⁷

³⁶ Daugman, J., ‘High confidence visual recognition of persons by a test of statistical independence.’, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 15(11), pp. 1148-1161, 1993

³⁷ Biometric Research – PRIP MSU website, <http://biometrics.cse.msu.edu/>

5.2.5 Hand vein pattern

This technology is based on comparison of vascular pattern images of the back or palm of a hand. The devices use a near-infrared light source to shine on the hand and a near-infrared optical sensor system to capture the reflected light. Since near-infrared absorption and scattering properties of tissue and blood differ,^{38 39} an image of the vein pattern is effectively captured. Image processing algorithms are used to facilitate template creation and comparison (see Figure 5-9).

Manufacturers claim that no non-biometric patterns can be enrolled, as extensive checking is done of whether or not an actual, living hand is presented, for instance by sensing the temperature pattern⁴⁰ or an active flow of haemoglobin through the person’s veins⁴¹. In general, such checking of ‘aliveness’ is referred to as ‘liveness detection’.

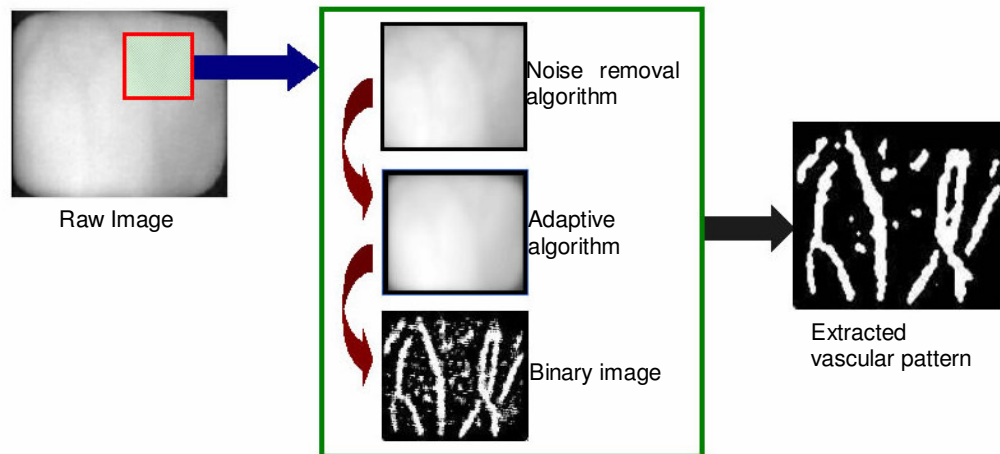


Figure 5-9: Hand vascular pattern extraction process flow⁴²

³⁸ Institute for Biodiagnostics website, Tissue Absorption, http://www.ibd.nrc-cnrc.gc.ca/english/spec_e_inVivo_absorption.htm

³⁹ UCL Department of Medical Physics & Bioengineering website, http://www.medphys.ucl.ac.uk/research/borl/research/NIR_topics/nirs.htm

⁴⁰ Tech-Sphere website, <http://www.tech-sphere.com>

⁴¹ Fujitsu Systems Business, ‘Fujitsu Announces Global Launch of its Contactless Palm Vein Authentication Technology’, 30 June 2005, available at http://www.fujitsu.com/th/en/news/recent/news_Palm_Vein.html

⁴² SynchrO website, <http://www.udc-synchro.co.jp/>

5.3 Forms of failure of biometric systems

The Common Criteria Biometric Evaluation Methodology Working Group (CCBEMWG)⁴³ has put together an extensive list of potential threats to a general biometric system. Figure 5-10 shows a schematic representation of a general biometric system and the locations of potential threats. The meaning of the number is explained in Table 5-2.

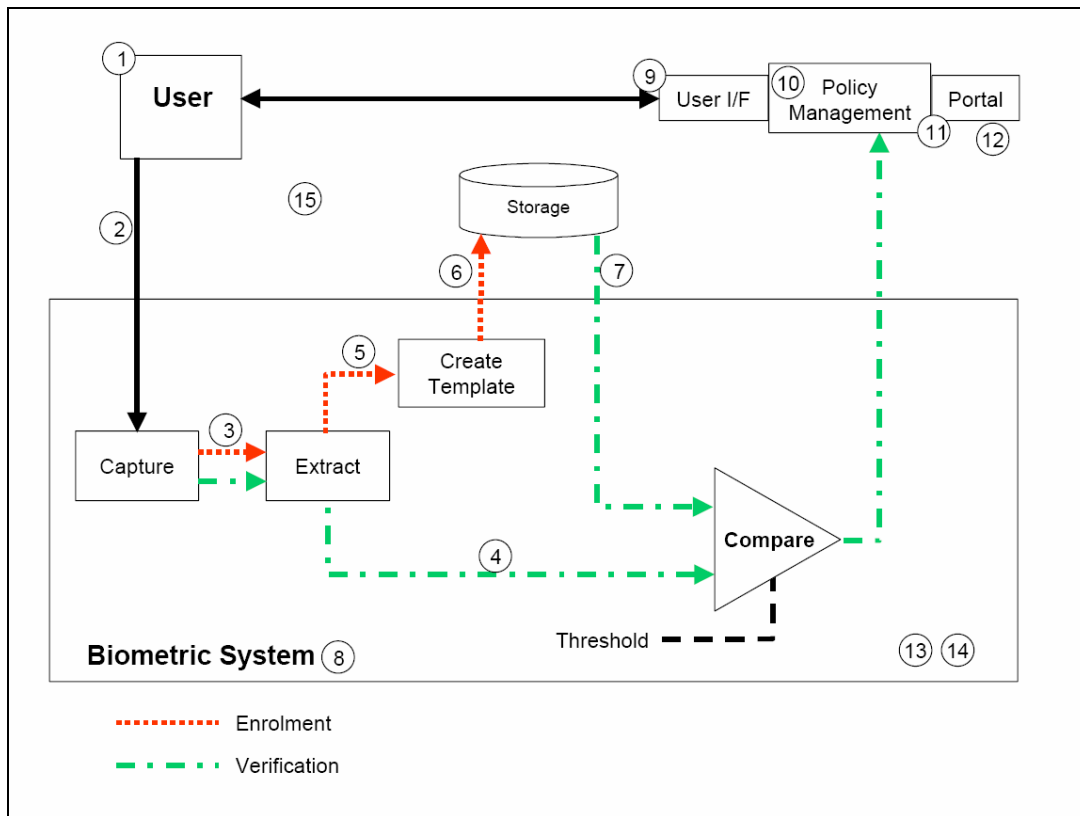


Figure 5-10: Simplified biometric system and potential threat locations⁴³

No.	Threat
1	User Threats. Authorised user provides own biometric sample, unknowingly, unwillingly (coercion), or willingly (collusion), to impostor
2	User / Capture Threats
3	Capture / Extraction Threats
4	Extraction / Comparison Threats during Verification

⁴³ Common Criteria Biometric Evaluation Methodology Working Group, ‘Common Criteria – Common Methodology for Information Technology Security Evaluation – Biometric Evaluation Methodology Supplement’, Version 1.0, August 2002

No.	Threat
5	Extraction / Template Storage Threats during Enrolment
6	Template Storage Threats
7	Template Retrieval Threats
8	Administrator / Resource Manager Threats
9	User / Policy Management Threats
10	Policy Management Threats
11	Threats to Policy Management / Portal
12	Portal Threats
13	Threats to all hardware components, e.g. Biometric sensor, portal hardware, integrated circuits, input / output hardware, computer, etc.
14	Threats to all software / firmware components
15	Threats to all connections (including network threats)

Table 5-2: General threats for biometric systems⁴⁴

Ideally, all threat locations should be analysed. However, the scope of our investigations is limited to the first two threat locations. For these threats, Table 5-3 lists a further breakdown of these locations.

No.	Threat
1	User Threats. Authorised user provides own biometric sample, unknowingly, unwillingly (coercion), or willingly (collusion), to impostor
1.1	Impostor covertly captures a biometric sample from authorised user, e.g. record voice, photograph face, etc.
1.2	Impostor steals a biometric sample from an authorised user e.g. cut off authorised user’s finger, or install fake biometric readers to capture biometric sample.
1.3	Authorised user knowingly provides own biometric sample to impostor (collusion)
1.4	Authorised user modifies own biometric sample to facilitate an impostor attack (collusion)
2	User / Capture Threats

⁴⁴ Common Criteria Biometric Evaluation Methodology Working Group, ‘Common Criteria – Common Methodology for Information Technology Security Evaluation – Biometric Evaluation Methodology Supplement’, Version 1.0, August 2002

No.	Threat
2.1	Impostor presents own biometric sample in a zero-effort attempt to impersonate <ul style="list-style-type: none"> (a) a randomly selected authorised user (for verification), (b) any authorised user (for identification), (c) a selected weak biometric template, or (d) an authorised user with a biometric sample similar to that of the impostor (e.g., a twin).
2.2	Impostor modifies own behaviour (e.g. voice, signature) or physiology (e.g. face, hand) in an attempt to impersonate <ul style="list-style-type: none"> (a) a selected authorised user, or (b) a selected weak biometric template.
2.3	Impostor presents an artificial biometric sample (e.g. fake fingerprint, voice recording) in an attempt to impersonate <ul style="list-style-type: none"> (a) a selected authorised user, or (b) a selected weak biometric template
2.4	Impostor presents a noisy, poor-quality, or null biometric sample in an effort to match a weak or regular-quality biometric template.
2.5	Impostor utilises a residual biometric image left on the biometric system (typically a latent fingerprint) in an attempt to impersonate the last authorised user.
2.6	Impostor presents own biometric sample after impostor’s biometric template has been: <ul style="list-style-type: none"> (a) provided on a forged personal data carrier e.g. smart card; (b) placed in the biometric system’s template storage database by illegal enrolment; (c) illegally added directly to storage database; or (d) illegally inserted directly into the comparison subsystem.
2.7	Impostor mounts a hill-climbing ⁴⁵ or other repeated-attempt attack that is not detected via audit trails.

Table 5-3: Breakdown of user and capture threats⁴⁶

More specifically, we have tested a number of biometric devices for weaknesses that show to be classifiable in threat categories 1.1, 1.3, 2.1, 2.3 or 2.6b.

⁴⁵ Hill-climbing attack: Attack in which artificially generated templates are input to the biometric template matcher. Using matcher feedback (such as matching score), the attack is repeated with each next input being a perturbation of the best matching template so far, until the matching score exceeds the acceptance threshold

⁴⁶ Common Criteria Biometric Evaluation Methodology Working Group, ‘Common Criteria – Common Methodology for Information Technology Security Evaluation – Biometric Evaluation Methodology Supplement’, Version 1.0, August 2002

5.4 Verification problems: biometric device technology

5.4.1 Evaluated devices

Fingerprint scanner sensor technology has a significant influence on the quality of images that can be extracted, as well as the possibilities for using fake fingerprints to fool the device. For most of the technologies mentioned earlier qualitative tests have been conducted to establish an overview of their strengths in terms of image quality and possibilities for fooling. Table 5-4 lists some basic information on the fingerprint scanners that have been evaluated.

Technology used	Company	Device model	DPI	Pixels	Label in Figure 5-11
Optical sensors:					
Frustrated Total Internal Reflection (FTIR)	Digital Persona	UareU4000	512	320x356	a
Surface Enhanced Irregular Reflection (SEIR)	BioCert	Hamster III (SecuGen FDU02 sensor)	500	260x300	b
Electro-optical	Security First Corp	Ethenticator 2500 USB	504	297x390	c
Touchless	TST	Bird Iii	500	256x360	d
Solid-state sensors:					
Capacitive	Precise Biometrics	100 SC	500	162x176	e
Electric field	Targus	DEFCON Authenticator PA460U (Authentec Entrépad AES 4000 sensor)	250	194x194	f
Piezoelectric	IdentAlink	UFIS210 (BMF BLP-100 sensor)	440	256x384	g
Thermal (sweep sensor)	IdentAlink	UFIS110 (Atmel FingerChip FCD4B14CC thermal sensor)	500	280x440	h
Other sensor:					
Ultrasonic	Ultra-Scan	Ultra-Touch 203	500	376x376	i

Table 5-4: Fingerprint scanners that were selected for evaluation

For the other selected biometric features the models displayed in Table 5-5 have been evaluated.

Biometric feature	Company	Device model	Label in Figure 5-11
Iris	Panasonic	Authenticam BM-ET100US	j
Hand geometry	IR Recognition Systems	HandKey II	k
Hand vascular pattern	Techsphere	VP-II	l

Table 5-5: Selected biometric devices for evaluation



Figure 5-11: The evaluated biometric devices (see also Table 5-4 and Table 5-5)

5.4.2 Image extraction using live fingers with various skin conditions

Figure 5-12 through Figure 5-15 show fingerprint images as captured by different scanners for various finger skin conditions. For each image of a certain skin type, the same finger is used. The images are displayed with proportions in accordance with the scanner DPI values.









Scanner sensor technology	Normal skin condition	Dry skin	Moist skin	Damaged skin with shallow valleys and broad ridges
FTIR: Digital Persona UareU4000				
SEIR: BioCert Hamster III (SecuGen FDU02 sensor)				

Figure 5-12: Fingerprint images of live fingers with different skin conditions as acquired by different commercial scanners




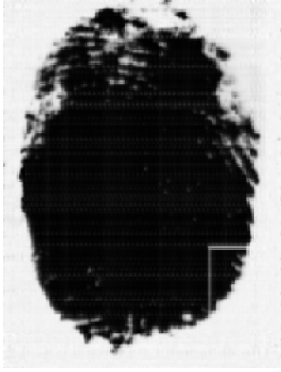




Scanner sensor technology	Normal skin condition	Dry skin	Moist skin	Damaged skin with shallow valleys and broad ridges
Electro-optical: Security First Corp Ethenticator 2500 USB				
Touchless: TST Bird Ili				

Figure 5-13: Fingerprint images of live fingers with different skin conditions as acquired by different commercial scanners








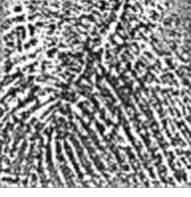




Scanner sensor technology	Normal skin condition	Dry skin	Moist skin	Damaged skin with shallow valleys and broad ridges
Capacitive: Precise Biometrics 100 SC				
Electric field: Targus DEFCON Authenticator PA460U (Authentec Entrépad AES 4000 sensor)				
Piezoelectric: IdentAlink UFIS210 (BMF BLP-100 sensor)				

Figure 5-14: Fingerprint images of live fingers with different skin conditions as acquired by different commercial scanners









Scanner sensor technology	Normal skin condition	Dry skin	Moist skin	Damaged skin with shallow valleys and broad ridges
Thermal (sweep): IdentAlink UFIS110 (Atmel FingerChip FCD4B14CC thermal sensor)				
Ultrasound: Ultra-Scan Ultra-Touch 203				

Figure 5-15: Fingerprint images of live fingers with different skin conditions as acquired by different commercial scanners

5.5 Threat level of biometric device spoofing

Most biometric devices can be fooled, also known as ‘spoofing’, using relatively simple means. This makes that these devices still require human supervision when used in high-security applications to ensure that this weakness is not exploited. Furthermore, it diminishes the forensic reliability of user traces in unsupervised biometric access control systems, as they could originate from fake biometric samples. The following paragraphs show the methods that have been tested.

5.5.1 Fingerprint spoofing

The following types of fake fingerprints were tested:

1. Gelatin fingerprint from silicone mould
2. Super Soft Plastic fingerprint (thin and thick layer version) from silicone mould
3. Wood glue fingerprint from digital image of fingerprint printed on sheet
4. Rubber fingerprint stamp from digital image of fingerprint

The first two methods require cooperation of an authorised user, as an actual finger is needed to make an impression in silicone. Methods three and four require a digital image of a fingerprint. For the spoofs made here, a rolled ink fingerprint was used as source, which was then digitised using a flatbed scanner. Alternatively, one could use conventional forensic methods to get a digital photograph of a residual fingerprint that an authorised user left on some object. This can potentially be used to steal a person’s fingerprint and enter a biometric system without cooperation of the authorised user.

The making of the moulds and thus the artificial fingerprints is described next.

Making the silicone mould

We used two-component low-viscosity silicone paste for making a mould (see Figure 5-16). This material captures the details of a fingerprint well, and can be used multiple times for making an artificial finger without getting damaged. The procedure entails mixing the two components in the right proportions quickly but thoroughly, and then pressing the finger into the mixture the same way one would press a fingerprint sensor. After holding still for a few minutes until the paste has dried and hardened, careful removal of the finger leaves a good quality mould.

Making a usable digital image of a fingerprint

Spoofing methods three and four require the digital image of the fingerprint to be binary. Digital photographs of a fingerprint residue made visible by standard forensic methods and scans of a rolled fingerprint are usually in colour or greyscale format, so some image processing must be done. For the scanned image of the rolled fingerprint we used an image editing package to change the brightness and contrast with -60 and +100, respectively, effectively binarising the image (see Figure 5-17). Depending on if the image is to be used as input for a mould or a stamp, it may have to be inverted and/or mirrored.

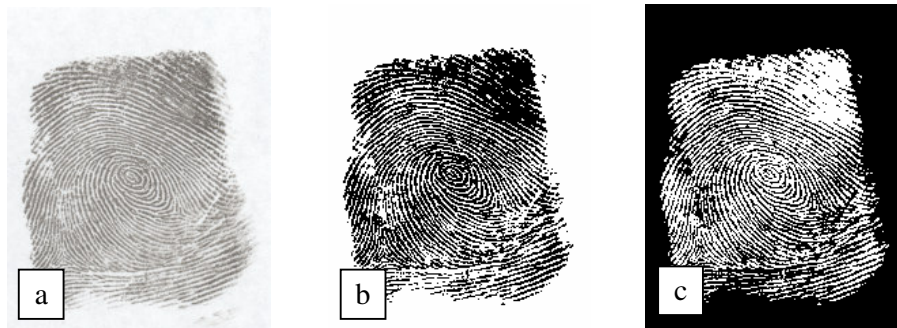
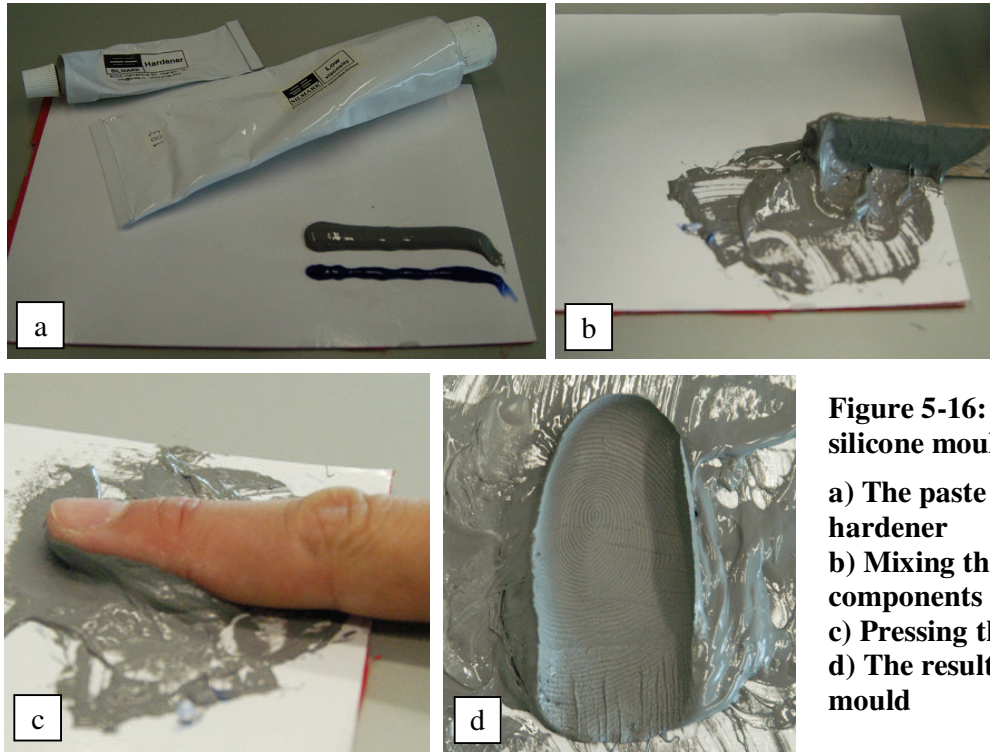


Figure 5-17: Processing a scanned image of a rolled ink fingerprint. a) The scan of the rolled fingerprint. b) The binarised image. c) The binarised and inverted image.

Making the gelatin fingerprint

Making the so-called ‘gummy fingers’ has been done extensively before^{47 48 49}. The method involves dissolving ‘kitchen-quality’ gelatin in near-boiling hot water and pouring it into a mould, such as the previously described silicone mould. When cooled down, the result is a flexible, transparent, yellowish cast of the finger. The main reason for using gelatin solution is that its electrical conductivity and moisture level resemble that of a human finger⁴⁷. Sensor technologies based on such finger properties are therefore usually also responsive to this material.

A solution of approximately 55% water and 45% gelatin was used. Dissolving such relatively high amounts of gelatin in water without getting bubbles takes some practice. Gentle stirring and repeatedly cooling down and heating up the solution (while keeping below boiling point) may be necessary to allow bubbles to escape the mixture.

Making the Super Soft Plastic fingerprint

Super Soft Plastic (see Figure 5-18) is a non-toxic polymer that comes as a whitish opaque liquid. After heating, it turns solid when cooled down to room temperature. The result is a soft, flexible, transparent and colourless plastic. It is typically used for creating fish lures, and may be found in some fishing shops.

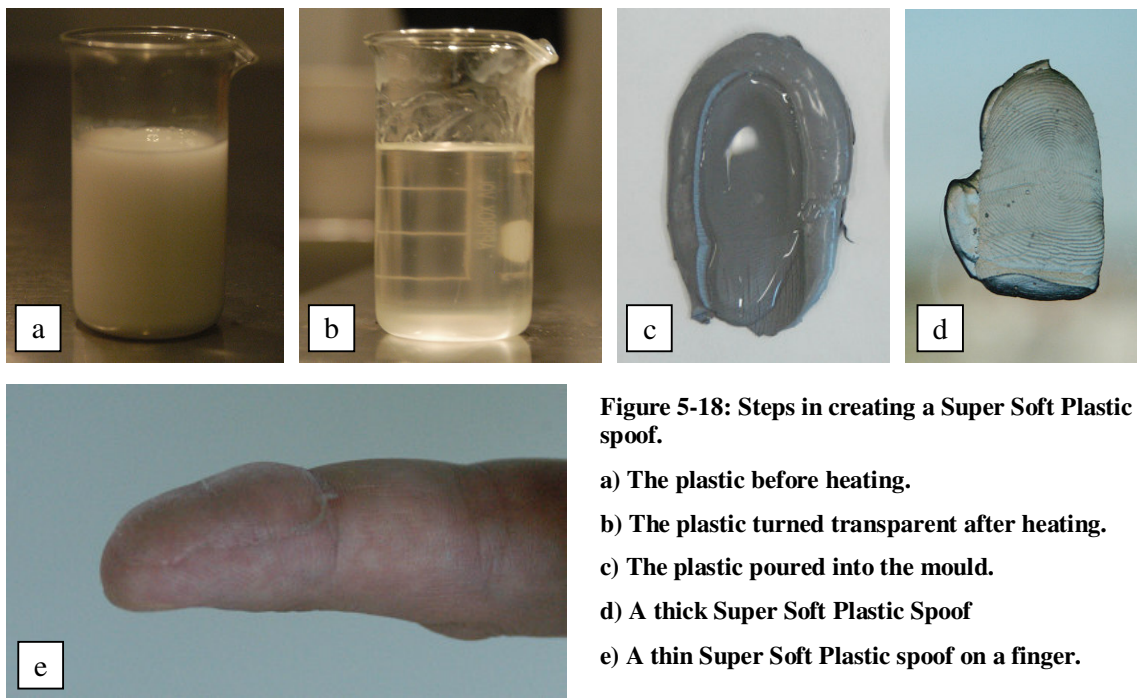


Figure 5-18: Steps in creating a Super Soft Plastic spoof.
a) The plastic before heating.
b) The plastic turned transparent after heating.
c) The plastic poured into the mould.
d) A thick Super Soft Plastic Spoof
e) A thin Super Soft Plastic spoof on a finger.

⁴⁷ Blommé, J., Evaluation of biometric security systems against artificial fingers, Master’s thesis LITH-
 ISY-EX-3514-2003, Department of Electrical Engineering, Linköping University, Linköping, Sweden, October
 2003

⁴⁸ Thalheim, L., Krissler, J., Ziegler, P.M., ‘Körperkontrolle - Biometrische Zugangssicherungen auf die
 Probe gestellt’, c’t 11/2002, page 114, available at <http://www.heise.de/ct/english/02/11/114/>

⁴⁹ Matsumoto, T., ‘Gummy Finger and Paper Iris: An Update’, October 2004, available at
<http://www-kairo.csce.kyushu-u.ac.jp/WISR2004/presentation12.pdf>

A small amount of Super Soft Plastic is heated in a microwave just until the liquid turns completely colourless and transparent. One must keep a constant eye on the substance while heating, as it can easily overheat and consequently burn, turning yellowish and lumpy, diminishing its usability. The heated plastic is then poured in the silicon mould and left some time to cool down and turn solid. For making a thin spoof, just pour in a small quantity and tilt the mould a bit to spread the liquid out over the mould surface.

Making the wood glue fingerprint

This technique is based on the fact that when printing with a laser printer, the toner forms a relief that is deep enough to be useful for making a fingerprint mould. Wood glue is an appropriate material for the fake fingerprint, as it can be smeared out in a thin layer, dries up transparently, and returns to its dried-up shape well after bending or stretching.

This spoof can be made as follows⁵⁰ (see Figure 5-19):

1. Print the binarised, inverted image of the fingerprint on a plastic sheet using a laser printer.
2. Smear out a thin layer of ordinary wood glue across the image.
3. Let it dry until the glue becomes transparent.
4. Carefully peel off the layer of glue
5. Cut the glue sheet to a size fitting your fingertip and stick it on. If it does not stick well enough by itself, use theatrical glue.

⁵⁰ Starbug, How to fake fingerprints, available at http://www.ccc.de/biometrie/fingerabdruck_kopieren.xml?language=en, October 2004

FIDIS

Future of Identity in the Information Society (No. 507512)

D6.1

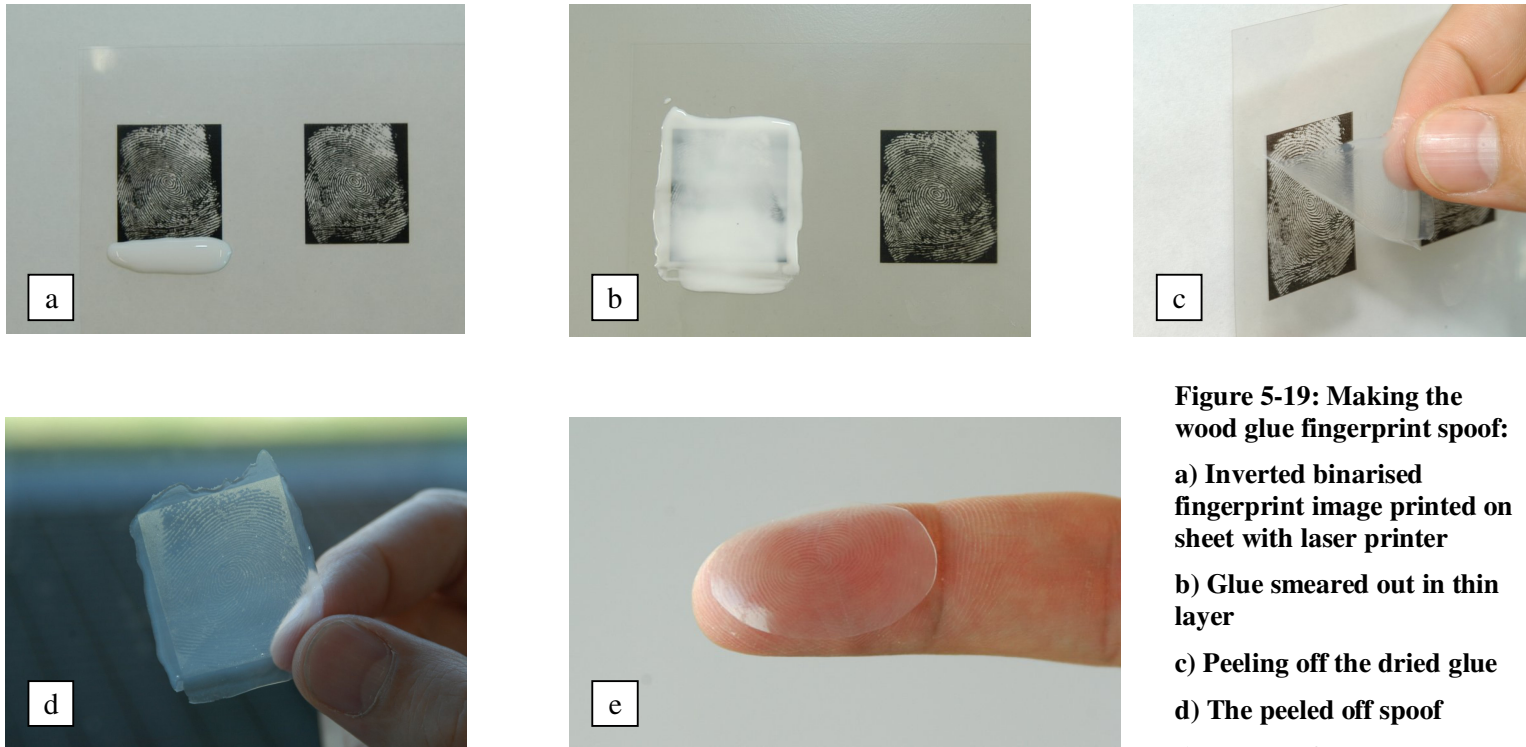


Figure 5-19: Making the wood glue fingerprint spoof:

- a) Inverted binarised fingerprint image printed on sheet with laser printer**
- b) Glue smeared out in thin layer**
- c) Peeling off the dried glue**
- d) The peeled off spoof**
- e) The spoof cut to proper size and stuck on fingertip**

Making the rubber fingerprint stamp

Professional stamp making machines used by stamp factories need only a digital, binary image as input for making a stamp. A laser with a fixed intensity burns away the appropriate parts by passing the surface of a rubber sheet to leave a relief of the input image, up to a precision of 1000 DPI (see Figure 5-20). The burn depth is determined by the movement speed of the laser. This speed is constant for a single stamp, so there can be no variation in the depth up to which the rubber is burnt away. A 25 Watt Trotec laser engraving machine was used to make the stamps.

For a stamp to be used directly on a sensor, a binary image of a fingerprint will do. If a mould stamp is to be made, the image must also be inverted and mirrored. We found, however, that the method is not particularly fit for making moulds, as only the surface of the protruding edges of the stamp is as smooth as the original material was, but the burnt out parts are somewhat irregular.

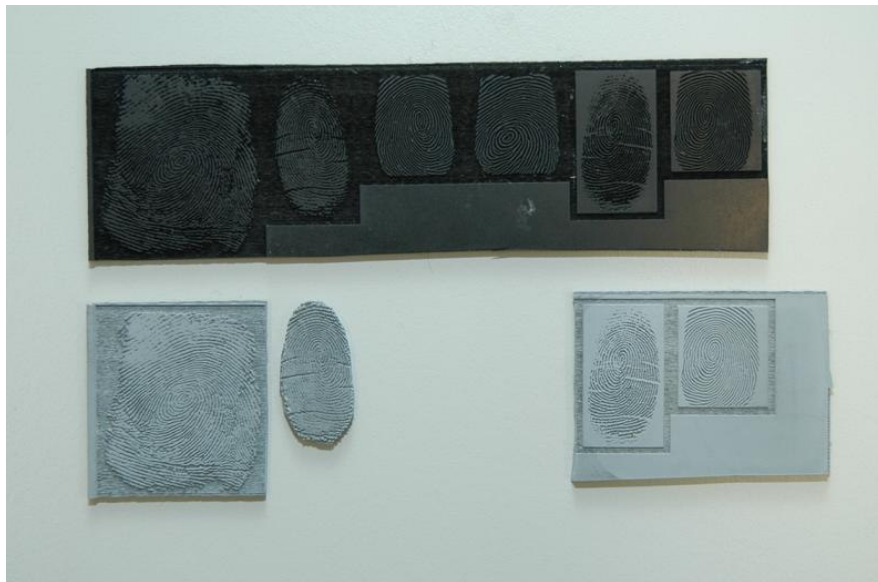


Figure 5-20: A set of rubber fingerprint stamp spoofs. The top sheet is made of synthetic vulcanised rubber, which is more resistant to chemicals than the natural vulcanised rubber the bottom sheet is made of. The two rightmost prints are negatives, for testing its fitness for use as a mould.

Given the spoofing techniques available, Table 5-6 through Table 5-14 show the images acquired from the tested scanners when presenting the artificial fingers. The cases where no images or unacceptable quality images were produced are not included.








 <p>Original live finger</p>	 <p>Material: Gelatin Mould: Silicone from live finger</p>	 <p>Material: Super Soft Plastic (thin layer) Mould: Silicone from live finger</p>	 <p>Material: Super Soft Plastic (thick layer) Mould: Silicone from live finger</p>
	 <p>Material: Wood glue Mould: Laser print on sheet</p>	 <p>Material: Grey rubber stamp Mould: Digital image of slapped ink fingerprint</p>	 <p>Material: Silicone Mould: Rubber stamp</p>

Table 5-6: Images from the Digital Persona UareU4000 FTIR scanner using fake fingerprints


 <p>Original live finger</p>	 <p>Material: Gelatin Mould: Silicone from live finger</p>	 <p>Material: Super Soft Plastic (thin layer) Mould: Silicone from live finger</p>	 <p>Material: Super Soft Plastic (thick layer) Mould: Silicone from live finger</p>
	 <p>Material: Wood glue Mould: Laser print on sheet</p>	 <p>Material: Grey rubber stamp Mould: Digital image of slapped ink fingerprint</p>	<p>(unacceptable quality)</p> <p>Material: Silicone Mould: Rubber stamp</p>

Table 5-7: Images from the BioCert Hamster III SEIR scanner using fake fingerprints



 <p>Original live finger</p>	 <p>Material: Gelatin Mould: Silicone from live finger</p>	<p>(no sensor response)</p> <p>Material: Super Soft Plastic (thin layer) Mould: Silicone from live finger</p>	<p>(no sensor response)</p> <p>Material: Super Soft Plastic (thick layer) Mould: Silicone from live finger</p>
	<p>(no sensor response)</p> <p>Material: Wood glue Mould: Laser print on sheet</p>	<p>(no sensor response)</p> <p>Material: Grey rubber stamp Mould: Digital image of slapped ink fingerprint</p>	<p>(no sensor response)</p> <p>Material: Silicone Mould: Rubber stamp</p>

Table 5-8: Images from the Security First Corp Ethenticator 2500 USB electro-optical scanner using fake fingerprints






 <p>Original live finger</p>	 <p>Material: Gelatin Mould: Silicone from live finger</p>	 <p>Material: Super Soft Plastic (thin layer) Mould: Silicone from live finger</p>	 <p>Material: Super Soft Plastic (thick layer) Mould: Silicone from live finger</p>
	<p>(no image available)</p> <p>Material: Wood glue Mould: Laser print on sheet</p>	 <p>Material: Grey rubber stamp Mould: Digital image of slapped ink fingerprint</p>	<p>(no image available)</p> <p>Material: Silicone Mould: Rubber stamp</p>

Table 5-9: Images from the TST Bird Iii touchless scanner using fake fingerprints



 Original live finger	 Material: Gelatin Mould: Silicone from live finger	(no sensor response) Material: Super Soft Plastic (thin layer) Mould: Silicone from live finger	(no sensor response) Material: Super Soft Plastic (thick layer) Mould: Silicone from live finger
	(no sensor response) Material: Wood glue Mould: Laser print on sheet	(no sensor response) Material: Grey rubber stamp Mould: Digital image of slapped ink fingerprint	(no sensor response) Material: Silicone Mould: Rubber stamp

Table 5-10 Images from the Precise Biometrics 100 SC capacitive scanner using fake fingerprints



 <p>Original live finger</p>	 <p>Material: Gelatin Mould: Silicone from live finger</p>	<p>(no sensor response)</p> <p>Material: Super Soft Plastic (thin layer) Mould: Silicone from live finger</p>	<p>(no sensor response)</p> <p>Material: Super Soft Plastic (thick layer) Mould: Silicone from live finger</p>
	<p>(no sensor response)</p> <p>Material: Wood glue Mould: Laser print on sheet</p>	<p>(no sensor response)</p> <p>Material: Grey rubber stamp Mould: Digital image of slapped ink fingerprint</p>	<p>(no sensor response)</p> <p>Material: Silicone Mould: Rubber stamp</p>

Table 5-11: Images from the Targus DEFCON Authenticator PA460U electric field scanner using fake fingerprints





 <p>Original live finger</p>	 <p>Material: Gelatin Mould: Silicone from live finger</p>	<p>(unacceptable quality)</p> <p>Material: Super Soft Plastic (thin layer) Mould: Silicone from live finger</p>	<p>(unacceptable quality)</p> <p>Material: Super Soft Plastic (thick layer) Mould: Silicone from live finger</p>
	 <p>Material: Wood glue Mould: Laser print on sheet</p>	 <p>Material: Grey rubber stamp Mould: Digital image of slapped ink fingerprint</p>	<p>(unacceptable quality)</p> <p>Material: Silicone Mould: Rubber stamp</p>

Table 5-12: Images from the IdentAlink UFIS210 piezoelectric scanner using fake fingerprints




 <p>Original live finger</p>	 <p>Material: Gelatin Mould: Silicone from live finger</p>	<p>(unacceptable quality)</p> <p>Material: Super Soft Plastic (thin layer) Mould: Silicone from live finger</p>	<p>(unacceptable quality)</p> <p>Material: Super Soft Plastic (thick layer) Mould: Silicone from live finger</p>
	<p>(unacceptable quality)</p> <p>Material: Wood glue Mould: Laser print on sheet</p>	 <p>Material: Grey rubber stamp Mould: Digital image of slapped ink fingerprint</p>	<p>(unacceptable quality)</p> <p>Material: Silicone Mould: Rubber stamp</p>

Table 5-13: Images from the IdentAlink UFIS110 thermal scanner using fake fingerprints

 <p>Original live finger</p>	 <p>Material: Gelatin Mould: Silicone from live finger</p>	 <p>Material: Super Soft Plastic (thin layer) Mould: Silicone from live finger</p>	 <p>Material: Super Soft Plastic (thick layer) Mould: Silicone from live finger</p>
	 <p>Material: Wood glue Mould: Laser print on sheet</p>	 <p>Material: Grey rubber stamp Mould: Digital image of slapped ink fingerprint</p>	<p>(unacceptable quality)</p> <p>Material: Silicone Mould: Rubber stamp</p>

Table 5-14: Images from the Ultra-Scan Ultra-Touch 203 ultrasonic scanner using fake fingerprints

Regarding the usefulness of the different spoofs for use in practical circumvention of biometric device functionality, the following can be concluded:

Gelatin:

- The only spoof that produced an acceptable result with all the tested scanners.
- Best overall image quality of all the spoofs, based on visual inspection. The touchless technology scanner does show extra highlights with a fresh gelatin print, which can give away the spoof.
- Durability is not very good. When kept in the open, it quickly dries and shrinks. When kept in a plastic bag, it lasts longer, but will become mouldy. Keeping it a refrigerator lengthens its lifetime.
- Gelatin is cheap and available in almost every supermarket. So this technology is available to anyone who wants it.
- It takes some practice to prepare the mixture properly. Care must be taken not to get bubbles in the mixture, as this will adversely affect spoof quality.
- In our tests, user cooperation was needed for the mould. Note that other methods are known that can use a digital image of a fingerprint as source⁵¹, thus only requiring a latent fingerprint.

Super Soft Plastic:

- Able to fool the popular ‘good image quality’ optical scanners, as well as the ultrasound scanner.
- Not able to fool the scanners that use electrical properties of the finger.
- The material is quite soft and flexible, deforming under pressure, making it less suitable for use with pressure sensitive fingerprint scanners. With the thermal scanner, this also has the effect that the friction when sweeping the sensor surface causes unacceptable distortions.
- Durability is good. Does not dry out or shrink.
- The thin layer version of the spoof is relatively inconspicuous when stuck on a fingertip. However, because of the transparency of the material, the optical scanners sometimes show a feint impression of the underlying structure, which gets more obvious the thinner the spoof is. Adding colorant may solve transparency problem, but this has not yet been tested.
- It is very easy to make this spoof.
- The material is not very expensive (about 15 Euro per litre) and is not very hard to find and order via fishing material shops on the internet.
- User cooperation is needed for mould preparation.

⁵¹ Matsumoto, T., ‘Gummy Finger and Paper Iris: An Update’, October 2004, available at <http://www-kairo.csce.kyushu-u.ac.jp/WISR2004/presentation12.pdf>

Wood glue:

- Able to fool the popular ‘good image quality’ optical scanners, as well as the ultrasound scanner
- Not able to fool the scanners that use electrical properties of the finger.
- Durability is good as long as it is not used. Moist will degrade the spoof, so care must be taken not to have the spoof on a warm or sweaty finger for too long.
- The thinnest, most inconspicuous of the spoofs.
- The basic materials are cheap and readily available. With some knowledge of basic image processing software and access to a laser printer, it is quite easy to prepare this spoof. The only potential difficulty will be to get a good quality binary image from a latent fingerprint.
- User cooperation not required. A digital image of the ridge pattern is all that is required, which can be extracted from fingerprint marks on objects using conventional forensic methods.

Rubber stamp:

- Able to fool all scanners except the ones that use electrical properties of the skin. One can, however, easily discern the spoof by visual inspection of the digital images.
- Fitness for use as a mould is not optimal. Surfaces that are burned away by the laser of the stamp machine are not completely smooth and even, which will translate in casts with uneven and unsmooth ridges. Also, when the mould is too deep, cast materials tend to remain stuck in the mould, resulting in even more uneven ridge structures in the cast.
- Durability is very good. They can be used over and over again.
- The fingerprint image that is needed can be made with some knowledge of basic image processing software. Many stamp makers allow online ordering of stamps, where stamp images can be uploaded, making access to the technology quite easy.
- Making stamps is not expensive. Prices are below 10 Euro for a stamp.
- User cooperation not required. A digital image of the ridge pattern is all that is required, which can be extracted from fingerprint marks on objects using conventional forensic methods.

5.5.2 Iris spoofing

The Panasonic iris scanner was used in conjunction with I/O Software SecureSuite XS Workstation version 4.5, which enables logging on to a computer using iris verification. A live iris was enrolled into the database and fake irises were presented to the camera. Our tests

confirm previous successful tests⁵² in which the basic iris scanner was fooled using a paper photocopy of an iris. We however used much lower resolution images than were thus far considered necessary.

Paper iris method

All that is needed is a black-and-white low-resolution image of the authorised user's iris printed on paper (see Figure 5-21). As the scanner does check for the presence of a retina reflection, the pupil must be cut out to allow the user to look through the hole when presenting the paper iris. When taking a photograph of the iris, care must be taken not to 'pollute' the iris region with reflections. One can photograph through a tube to get a good result, and when the photo is taken from the front, any flash reflection will be inside the pupil region.



Figure 5-21: Original live iris and the paper spoof

In the tests, irises from both a 6 MegaPixel portrait photograph and a 6 MegaPixel close-up of the eye were used, which after rescaling to actual size resulted in a 240 and 500 ppi image, respectively. The images were printed using 600 dpi laser printer. After some practice, it was quite easy to pass the system using the fake irises, especially with the 500 ppi version.

To test the usability of old photographs, a similar test was also done using an analogue photograph of the authorised user from his childhood (from over 20 years ago). The photo was scanned to digital format and slightly brightened to make the details stand out more. The paper spoof created with this image was also accepted for verification.

5.5.3 Hand geometry spoofing

Our tests have shown that the HandKey II (Figure 5-23a) can in principle be fooled using something other than an actual hand, when security level is set somewhat below the factory setting. Furthermore, an unauthorised user with approximately the same hand size as the authorised user scores reasonably well, confirming the well-known fact that hand geometry uniqueness can be an issue (see also FIDIS Deliverable 3.2⁵³).

⁵² Thalheim, L., Krissler, J., Ziegler, P.M., 'Körperkontrolle - Biometrische Zugangssicherungen auf die Probe gestellt', c't 11/2002, page 114, available at <http://www.heise.de/ct/english/02/11/114/>

⁵³ FIDIS Deliverable 3.2: 'A study on PKI and biometrics', July 2005, available at <http://www.fidis.net>

Paper hand method

The image extraction method used in the HandKey II (see also section 5.2.4) suggests that it does not need to be presented with an actual 3D hand for getting a valid result, as only the side views are captured. Furthermore, judging from Figure 5-22, the influence of the side view is not expected to be so big. The figure shows that the side view of the hand accounts for a relatively small part of the information captured by hand geometry recognition devices.



Figure 5-22: Typical image captured by a hand geometry recognition device⁵⁴

Tests show that a top view silhouette of a hand cut out in paper can indeed be enough to pass the verification check of the device, albeit at a lowered security level. When verifying a user, the device shows matching scores, up to a value of 250, lower being better. A rejection threshold can be set. The default rejection value is 100. In order to facilitate testing matching scores, the rejection threshold was set to 250. Note that this setting is not representational of practical use of the device.

The paper hand can be made as follows (see Figure 5-23e):

1. Measure the sizes and relative positions of the guidance pegs
2. Precisely draw the pegs' in the proper configuration using drawing software and print it on a transparent sheet (alternatively, print it on paper, then copy it on sheet)
3. Make a photocopy of the authorised user's hand with a photocopier. Use the sheet with the peg configuration to properly position the hand and fingers on the copier.
4. Cut out the paper hand.

An important thing to acknowledge during testing is that user templates are updated using data from the latest successful login. This means that the more often the fake hand is accepted for verification, the better the scores get. Therefore a fresh enrolment of the live hand was done each time the paper hand was presented.

⁵⁴

Recognition Systems, Inc., European Patent EP0209317, 'Identification Apparatus', 1986

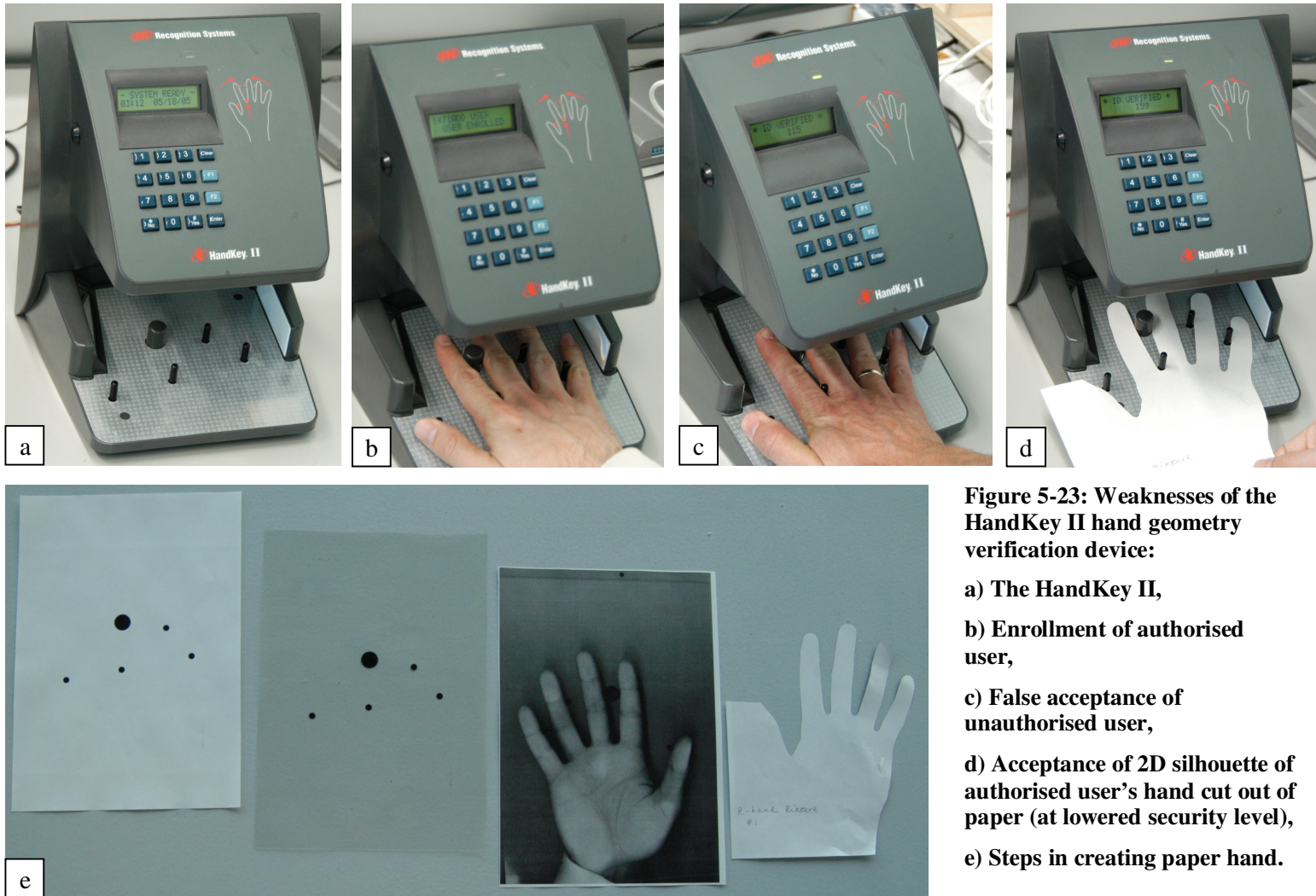


Figure 5-23: Weaknesses of the HandKey II hand geometry verification device:

- a) The HandKey II,**
- b) Enrollment of authorised user,**
- c) False acceptance of unauthorised user,**
- d) Acceptance of 2D silhouette of authorised user’s hand cut out of paper (at lowered security level),**
- e) Steps in creating paper hand.**

Table 5-15 and Figure 5-23 show results of the qualitative tests (limited amount of tests).

Enrolment with	Verification with	Best score achieved (on first try after enrolment)
Live hand	Same hand	8
Live hand	Unauthorised similar hand	115
Live hand	Paper hand	159

Table 5-15: Results of testing the HandKey II weaknesses

It is expected that the scores can still be improved by cutting a more accurate representation of the hand top view. Also, adding the side view silhouette to the paper hand is expected to improve the scores. These possibilities are currently under investigation.

5.5.4 Hand vascular pattern spoofing

In our experiments we were not successful in fooling the TechSphere VP-II device at its standard settings. The device can however be partially fooled by non-biometric patterns. Configurations which have achieved this are:

- with liveness detection turned totally off, a paper print-out of the vascular pattern of an authorised user can be enough to pass the verification
- with liveness detection turned totally off, a paper print-out of a person’s vascular pattern can be enrolled. Then, when turning the liveness detection back on, the actual person can log into the system using his own hand.
- with liveness detection turned on, a non-biometric pattern can be enrolled and verified, in this case a section of a latex glove wrapped around a bottle. Thus far all attempts to fool the liveness detection with a copy of a vascular pattern have failed.

These methods are elaborated below:

Vascular pattern print-out method (partial spoof)

Basically, one must create a grey-and-white copy of the pattern of the veins on the back of the hand. Some people have clearly visible veins that lie close to the surface of the skin, in which case a normal digital photograph of the top view of the hand in enrolment attitude will do as a starting point (see Figure 5-24a). In that case the following procedure can be followed:

1. Draw reference dots on the back of the hand at known distances from each other. These can be used later to scale the photograph to the right size.
2. Take a photograph of the top view of the back of the hand (Figure 5-24a). The hand should have the same attitude as it would have when enrolling.

3. Use image processing software that can work with layers to manually trace the vein pattern (Figure 5-24b).
4. Print just the drawn layer in the actual size (scale the picture using reference dots). Colour contrast of lines and background should not be too great. Grey value 128 on a white background works fine (Figure 5-24c).

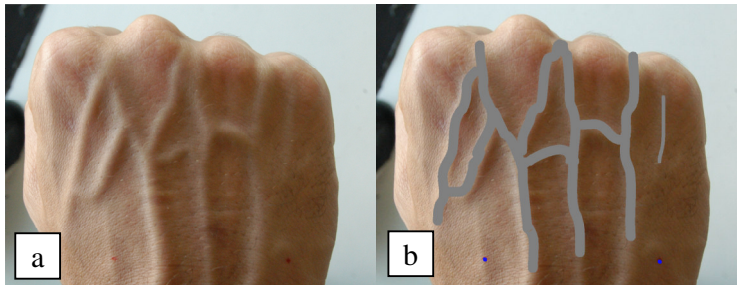


Figure 5-24: Obtaining a vascular pattern using a digital camera. a) Image of the back of a hand shot in daylight using a common digital photo camera. b) Visible veins manually traced using image processing software. c) The drawn layer ready for printing

If the veins are not sufficiently discernable in visible light, a camera with ‘nightshot’ function can be used. Such cameras use a near-infrared lamp to illuminate the target and a sensor array that is sensitive to near-infrared light to capture the reflecting rays. The quality of the nightshot function varies with camera type. In this experiment, a Sony DCR-TRV9E Digital Video Camera Recorder was used with good results. The spoof can be made as follows:

1. Cover the camera-mounted near-infrared lamp with some sheets of tissue (Figure 5-25a). This blocks a portion of the light, which is necessary to prevent spots of over-exposure that make post-processing more difficult.
2. In a dark room, take a shot of the top view of the back of the hand using the nightshot function of the camera. The hand should have the same attitude as it would have when enrolling (Figure 5-25b). One can include a measuring stick at the same height as the back of the hand to the shot to facilitate scaling later on.
3. Use either the previously discussed tracing method or a sequence of image processing filters to obtain a two-colour representation of the vascular pattern (Figure 5-25c). An example of a filter sequence that was used in this test is:
 - Apply a Gaussian blur on the image. Use a blur radius large enough to make the details fade. We used a radius of 25 pixels for a 720 by 576 pixel image.
 - Subtract the blurred image from the original. This reduces the more global differences in intensity that may be present due to uneven lighting conditions.
 - Binarise the image using a grey value threshold that leaves the veins well visible
 - Apply a Gaussian blur on the image. Use a blur radius large enough to make pixels that make out the veins connect, but small enough to keep the vein lines standing out. We used a radius of 3 pixels for a 720 by 576 pixel image.
 - Binarise the image again using a grey value threshold that leaves the veins well visible
 - Lower the contrast by changing black to grey (for example grey value 128)
4. Scale the image so it represents the actual size and print the resulting image.

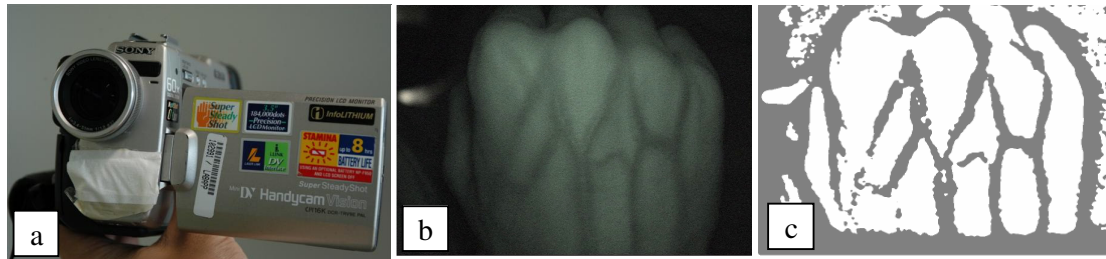


Figure 5-25: Obtaining a vascular pattern using a nightshot camera. a) Handycam with nightshot function. The near-infrared lamp is covered with tissues to diminish bright spots when using the camera at close range. b) Image of the back of a hand shot in the dark using the nightshot camera. c) Two-colour vascular pattern extracted from nightshot image using image processing techniques

The paper pattern can be stuck on someone’s hand or anything else, such as a bottle (Figure 5-27). When presenting the spoof to the vascular pattern scanner, care must be taken to match the pattern position with the position of original live hand, as the device is very sensitive to shifting of the pattern.

Latex glove on bottle method (partial spoof)

This method entails nothing more than placing a cylindrical object, such as a bottle or a can, into a powder-free latex examination glove (see Figure 5-26). Even when using an evenly textured object, the spoof has to be put in the exact same position each time or else enrolment or verification will fail.

Drawing a pattern on the glove with markers, or sliding a pattern copied on paper between the glove and the bottle, caused the enrolment to fail.

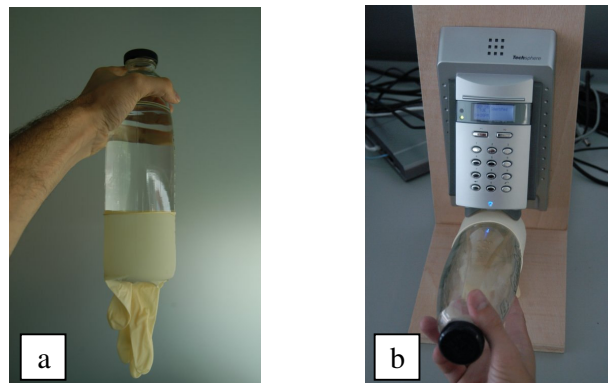


Figure 5-26:a) Latex glove on bottle. b) The latex glove identified (liveness detection on).

Table 5-16 shows which types of spoofing were successful with different liveness detection settings. Figure 5-27 shows images of the actual tests.

It can be concluded that the device does not live up to its manufacturers’ liveness detection claims, as cold, static, inanimate objects can be enrolled and verified. It implies that the device interprets reception of certain types of static patterns of reflected near-infrared light as being caused by a live hand. Experiments are ongoing concerning determination of the properties of such patterns and potential materials and contrast patterns that may improve the spoof. Thus far, however, the ‘liveness detection’ algorithms have detected the attempts of fooling the device using copies of vascular patterns.

Enrolment liveness detection	Verification liveness detection	Enrol vascular pattern copy, verify with same	Enrol vascular pattern copy, verify with live vascular pattern	Enrol live pattern, verify with vascular pattern copy	Enrol latex glove on bottle, verify with same
Off	Off	successful	successful	successful	successful
On	Off				successful
Off	On		successful		successful
On	On				successful

Table 5-16: Vascular pattern recognition spoofing results for different liveness detection settings

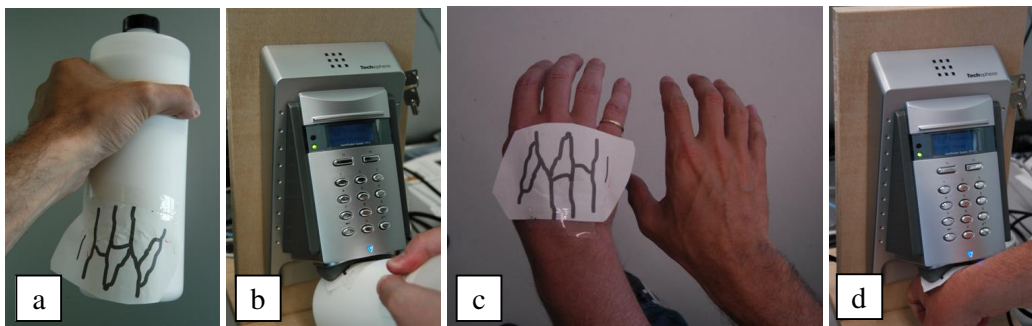


Figure 5-27: Vascular pattern spoofs effective with liveness detection turned off. a) The copy of a vascular pattern stuck on a bottle. b) The bottle spoof verified as an authorised user. c) The copy of a vascular pattern stuck on a hand (left), next to the original hand (right) of an authorised user. d) The hand spoof verified as the authorised user

5.6 Conclusion

Concluding, it is evident that the current state of the art of biometric devices leaves much to be desired. A major deficit in the security that the devices offer is the absence of effective liveness detection. At this time, the devices tested require human supervision to be sure that no fake biometric is used to pass the system. This, however, negates some of the benefits these technologies potentially offer, such as high-throughput automated access control and remote authentication.

The independent testing of biometric devices is still non-trivial as manufacturers tend to sell their products for more than they can achieve. The latter can give a false sense of security, adversely affecting actual security if not recognised in time. It is an issue that we encounter in many forms of technology today: if it can be cracked, it will be cracked. Accepting this would need a different attitude of manufacturers, in which more of what is going on inside the device and the accompanying software is made public. It would allow potential users of biometric systems to better judge the fitness of such systems for their particular purposes.

From a forensic point of view, care should be taken when drawing conclusions from information extracted from access control systems that use biometric devices. The possibility that the system was compromised, consequently falsely linking persons to events, should be examined or at least noted in the forensic examination report.

6 Overview of case law and acceptance of electronic evidence in court

6.1 What is forensic evidence?

The determination of identity is the principal aim of identity systems. In forensic science, the determination of identity can take the form of (1) establishing an identity of origin between two objects and (2) determining the nature of a specimen of evidence. The first category is typically the more significant one because it contributes to the final determination of the value of the evidence. It is, for example, more valuable to be able to say that two hairs belong to the same head, than to say that both hairs are human in origin.

The central task of the forensic investigator is to establish personal identity. Supplementary to this task is the identification of physical objects that may, in turn, contribute to the desired personal identification.⁵⁵ Physical evidence can therefore be divided into biological and non-biological evidence. The advent of computers and the phenomenal growth of their use have given rise to a second category, apart from physical evidence, known as digital evidence.

Another relevant distinction is the difference between direct and indirect evidence. Indirect evidence is often referred to as circumstantial evidence and is frequently confused with weak evidence. While a confession may or may not be true, it is still considered direct evidence. And, however rare the DNA profile is, its presence still does not prove that the suspected committed the murder, nor does it tell us in most cases when the material was deposited at the crime scene; in many cases it simply indicates the presence of the suspect at some time at a location connected with the crime. Depending on the circumstances of the crime, this may be very convincing, but that does not render it direct evidence.⁵⁶

Generally, identification is defined as the determination of the physical or chemical identity of a substance with as near absolute certainty as existing analytical techniques will permit. It is seen as defining the physiochemical nature of an evidence item, without a specific reference item.⁵⁷

The ultimate aim of the identification process is individualisation.⁵⁸ A definition of individualisation is given by Tuthill: “The individualisation of an impression is established by finding agreement of corresponding individual characteristics of such number and significance as to preclude the possibility (or probability) of their having occurred by mere coincidence, and establishing that there are no differences that cannot be accounted for.”⁵⁹ For forensic scientists, individualising an object means that it is possible to distinguish this object from all other possible objects.

⁵⁵ P. KIRK, *Crime investigation*, 1st ed., New York, Interscience, John Wiley & Sons, 1953.

⁵⁶ K. INMAN and N. RUDIN, *Principles and practice of criminalistics, the profession of forensic science*, A volume in the Protocols in Forensic Science Series, Boca Raton, CRC Press LLC, 2000, 102.

⁵⁷ K. INMAN and N. RUDIN, *Principles and practice of criminalistics, the profession of forensic science*, A volume in the Protocols in Forensic Science Series, Boca Raton, CRC Press LLC, 2000, 115.

⁵⁸ P.L. KIRK, “An ontology of criminalistics, the journal of criminal law”, *Criminology and Police Science*, 1963, 54, 235 – 238.

⁵⁹ H. TUTHILL, *Individualisation: principles and procedures in criminalistics*, Salem, Lightning Powder 1994, 21.

6.2 The collection of evidence

6.2.1 Admissibility of the evidence

The first vital question that needs to be answered is that of the legal admissibility of the evidence; one must first examine whether certain types or means of evidence are admissible or receivable. Two systems can be distinguished: firstly the system of the freedom of evidence, where the accent is put on the freedom of appreciation of the judge and the second one is the system of legality of the evidence, where the stress lays on the risks of judicial error or on the respect of the accused. Outside these two systems regimes exist where the evidence is even more restricted.

6.2.2 A. Freedom of evidence

There are systems that favour a very wide appreciation of the principle of the freedom of evidence, but not an absolute application. The general rule is that of the freedom of the judge, which is based on 'pure instinct', 'a pure intuition', on 'the voice of his conscience', but naturally this rule has its limits.⁶⁰

The rule is accepted practically everywhere, but it is expressed in different ways:

A very revealing example is art. 427 of the French CPP (Criminal Procedural Code), which reads: "Except in cases where the law rules differently, offences may be established by any means of evidence."

Art. 125 of the Portuguese CPP quite similarly states that all evidence, which has not been forbidden by law, is admissible.

The Belgian point of view is comparable. Although the code of criminal procedure enumerates various types of evidence (art. 154) it is accepted that the judge may agree to any kind of evidence, which the parties may put forward.

In Italy, art. 189 of the CPP permits the judge to accept any evidence which is not regulated by law so as to evaluate the case on a well-informed basis.

The principle of freedom is however not synonymous with arbitrary judgement or with disarray/disorder. Though free, the judge has to give a reason for his decision and has to do so solely on the basis of evidence, which has not been rejected. As the Italian doctrine lays down, it would not be possible to 'recuperate' evidence which was forbidden or illegal and therefore unusable because of an intimate conviction. It is almost a limit on the judge's freedom.

Limits on the freedom of the judge

1. The existence of summonses obliging the judge to convict. In France and Belgium one distinguishes ordinary summonses, which are simply statements that leave the judge all his freedom. Summonses will only stand until the contrary is proven, since they will only be withdrawn if no proof is brought forward. Finally, summonses are valid

⁶⁰ The Portuguese code invokes on this behalf that the judge will judge according to 'the rules of his experience' (art. 127).

Future of Identity in the Information Society (No. 507512)

until they may be found fraudulent upon which an action for forgery may be introduced.

2. The theory known as ‘corroboration’, as a result of which the judge can only convict someone if there are at least two or more pieces of evidence. Corroboration is accepted in Scotland as a general rule but only exceptionally in England. In the Netherlands, the judge cannot use confessions obtained by the police if they are not accompanied by other evidence. An extra-judiciary confession alone is not sufficient (art. 341 Code of Criminal Proceedings). In Portuguese law, the ‘technical judgement’ of an expert may not be overridden by the judge (art. 163 of the CPP) unless the latter can justify his objection on a technical basis or if he challenges the basis of the facts used by the expert. This is a way of obliging the judge – generally an amateur – to follow the expert who is a professional.⁶¹

6.2.3 B. Legality of the evidence

Art. 339 of the Dutch law (Code of Criminal Proceedings) lists all accepted types of evidence: the observations of the judge himself, declarations by the suspect and the witnesses, statements by experts, and any documents presented in evidence. This is an exhaustive account meaning no other types of evidence are allowed.

The German law includes the declarations of the accused and the witnesses, statements of experts, ‘view of something’ (means of proof which consists of what can be perceived by the senses at the crime scene) and also documents (arts. 48, 71, 72, 85, 86, 92, 249 and 256).

In practice however, these two systems of law are moving towards a system of freedom of evidence.

6.2.4 C. Countries where evidence is even more restricted

This category mainly concerns countries of common law. The rules dealing with the admission or exclusion of evidence only concern the question of the guilt of the accused. When it comes to the determination of the sentence in the second part of the trial, all evidence is admissible, even that which has been obtained by illegal means.⁶²

In the United States, the law defines evidence only by its relevance. Relevant evidence is admissible; irrelevant evidence is inadmissible.⁶³

⁶¹ J. PRADEL, “Criminal evidence” in J. F. NIJBOER and W. SPRANGERS (eds.), *Harmonisation in forensic expertise, an inquiry into the desirability of and opportunities for international standards*, Series criminal sciences, Amsterdam, Thela Thesis, 2000, 428 – 429.

⁶² In these countries namely hearsay evidence or evidence given by a witness before the judge about events of which he has not personally been a witness or evidence he has obtained by a third party who did not appear before the judge is forbidden. Also excluded is the accused’s bad reputation, whether it concerns his criminal record or dishonest acts committed in the past for it is thought that such evidence would negate the presumption of innocence and would incline the judge to allow a guilty verdict too easily. A third exclusion, which appears to be inherent to the USA, deals with admissions made by the accused during plea-bargaining with the prosecutor during which he admitted his guilt. This prohibition is intended to make negotiated settlements easier. J. PRADEL, “Criminal evidence” in J. F. NIJBOER and W. SPRANGERS (eds.), *Harmonisation in forensic expertise, an inquiry into the desirability of and opportunities for international standards*, Series criminal sciences, Amsterdam, Thela Thesis, 2000, 417 – 418.

⁶³ Article I and Article IV of the U.S. Federal Rules of Evidence (1999). Rule 104(b): “Relevancy conditioned on fact. When the relevancy of evidence depends upon the fulfilment of a condition of fact, the court shall admit it upon, or subject to, the introduction of evidence sufficient to support a finding of the fulfilment of the condition.” Rule 401: “Definition of ‘relevant evidence’. ‘Relevant evidence’ means evidence having any

6.3 The taking of samples

Taking samples from a person is considered to be a special kind of search. The regulations concerning this kind of evidence vary.

In the United Kingdom, the provisions of the Police and Criminal Evidence Act of 1984 allow the request to a suspect for a sample if accompanied by a form of caution under the Code of Practice for Identification of Persons by Police Officers.

Intimate samples may only be taken with the consent of the person concerned. They are defined as being blood, semen or any other tissue fluid, urine, pubic hair, a dental impression and a swab taken from a body orifice other than the mouth.⁶⁴ Whenever those samples are concerned, the authorisation may only be granted if there are reasonable grounds for suspecting the involvement of the person in a recordable offence, on the condition that the sample will tend to confirm or disprove his involvement.⁶⁵ Therefore, if the police wish to obtain a sample of blood for the purpose of confirming or disproving that person's involvement in an offence, they may only do so upon his consent.⁶⁶ The refusal of the suspect to allow such a sample to be taken cannot be directly overridden, but there is a sanction for refusal 'without good cause'. In that case, the judge or jury may consider the refusal as an indication of guilt.⁶⁷

Even if the suspect does not consent, a DNA analysis may be made from a non-intimate sample like a hair or saliva because developments in technology have enabled forensic scientists to extract DNA samples from hair and saliva. Therefore, while there may be substantial issues of self-incrimination involved in the non-consensual taking of samples, the question of whether there is an assault upon bodily integrity is arguably less substantial than in case of intimate searches.

tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence." Rule 402: "Relevant evidence generally admissible; irrelevant evidence inadmissible. All relevant evidence is admissible, except as otherwise provided by the Constitution of the United States, by Act of Congress, by these rules, or by other rules prescribed by the Supreme Court pursuant to statutory authority. Evidence which is not relevant is not admissible." Rule 403: "Exclusion of relevant evidence on grounds of prejudice, confusion or waste of time. Although relevant, evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence."

⁶⁴ Bodily samples can be classified as either 'intimate' or 'non-intimate' samples. In the United Kingdom, intimate samples are defined in the Police and Criminal Evidence 1984 as being blood, semen or any other tissue fluid, urine, pubic hair, a dental impression and a swab taken from a body orifice other than the mouth (section 65 PACE). This definition results in the fact that hair and saliva are considered to be non-intimate samples.

⁶⁵ The Police and Criminal Evidence Act 1984, section 62, provides for the taking of what is termed 'an intimate sample' from a person in police detention with the authorisation of an officer of at least the rank of superintendent and with the consent of the suspect. Reasonable grounds must exist for the authorisation and both these grounds and the relevant consent must be furnished in writing. 'Intimate sample' is defined in the Act and includes blood, semen and saliva. Such samples other than urine or saliva may only be taken by a registered medical practitioner.

⁶⁶ Police and Criminal Evidence Act 1984 section 62.

⁶⁷ Police and Criminal Evidence Act 1984, subsection 62(10) provides that, in determining whether a person is guilty of the offence charged, a court or jury may "draw such inferences from the refusal as appear proper; and the refusal may, on the basis of such inferences, be treated as, or as capable of amounting to, corroboration of any evidence against the person in relation to which the refusal is material." There has been challenge of the permissibility of drawing such inferences. However, in *Murray v. United Kingdom* (1996, 22 EHRR 29), the European Court of Human Rights held that there was no violation of Article 6 so long as the conviction was not based solely or mainly on the accused's silence or refusal.

Future of Identity in the Information Society (No. 507512)

Even when intimate samples are deemed necessary to prove involvement in an offence, such material may be voluntarily surrendered by the holder and it is then admissible against an accused as evidence obtained through consensual search. For example in the case of *R. v. Singleton*, a dentist handed dental records and the dental impression of a tooth taken from one of his patients over to the police. The patient was a murder suspect and the evidence assisted in convicting him because the dental impression matched the bite marks on the victim.⁶⁸

In Italy, sampling is not only prohibited, but in case of refusal the judge may not draw any negative conclusion.

In Germany sampling is possible – and may be ordered by the examining magistrate or by the public prosecutor or, in urgent cases, by the police – without the permission of the person concerned, unless by doing so a risk of health is incurred or if the medical intervention is a serious one.

In Canada sampling is forbidden except in certain special cases, e.g. the sampling of blood or urine of a person suspected of having driven a car under influence.⁶⁹

In Australia, the Crimes Act 1900 permits a police officer to search any person in lawful custody upon a charge of committing an offence and “take from the person anything found upon that search”. A search is only allowed when there are reasonable grounds of believing an examination will afford evidence and the Act prescribes the circumstances in which a legally qualified medical practitioner has to make a reasonable examination of the suspect.⁷⁰

6.4 Admissibility of expert’s opinion in court

6.4.1 The risks inherent in forensic evidence⁷¹

The first risk is that the scientific theory on which the expert’s opinion is based is wrong.

The second risk is that the scientists deliberately ‘cook’ their results.

⁶⁸ *R. v. Singleton* 1995 *Cr. App. R.*430. Lord Justice Farquharson made the following comment with regard to the case: “The object of the Police and Criminal Evidence Act is to protect disclosure of confidential personal records. It seems clear that the person to be protected from disclosure is not the suspect in any particular case, but the person who has acquired or created the record. Accordingly, if that person voluntarily discloses the record he does not seek or require the protection given by the Act to that class of record.” Ultimately, the decision about whether the police can gain access to a pre-existing intimate sample taken from a suspect rests not with that suspect, but with the medical practitioner holding the excluded material. It is the misfortune of the person under investigation that he had previously sought medical assistance and that the practitioner concerned has made a moral judgement in favour of disclosure to the police. This could be compared to the public safety exception in legal privilege such as exists in Canada and in the U.S. In those countries the exception applies where there is an imminent risk of serious bodily harm or death to an identified person or group of persons. In England and Wales, this exception has also been applied in respect of third parties such as psychiatrists (*W. v. Egdell* 1990, *ALL ER* 835).

⁶⁹ J. PRADEL, “Criminal evidence” in J. F. NIJBOER and W. SPRANGERS (eds.), *Harmonisation in forensic expertise, an inquiry into the desirability of and opportunities for international standards*, Series criminal sciences, Amsterdam, Thela Thesis, 2000, 422.

⁷⁰ Section 353A of the Crimes Act 1900, see also Section 81 of the Police Offences Act 1953, Sections 6 and 7 of the Criminal Process (Identification and search procedures) Act 1976, Section 259 of the Criminal Code Act 1899 and Section 145 of the Police Administration Act 1984.

⁷¹ J. SPENCER, “Evidence and Forensic Science” in J. F. NIJBOER and W. SPRANGERS (eds.), *Harmonisation in forensic expertise, an inquiry into the desirability of and opportunities for international standards*, Series criminal sciences, Amsterdam, Thela Thesis, 2000, 549 – 552.

Future of Identity in the Information Society (No. 507512)

The third risk is that the scientists, though honest, have done their work incompetently. The scientist may have used unreliable methods without necessarily realising it. Sometimes the incompetence results from the way in which the scientist interprets the results of the tests, rather than the way in which he conducts the examination. The scientist may even be incompetent by failing to take account of some important extra factor that could change his conclusion radically.

Lastly, forensic evidence involves a danger that has nothing to do with the honesty or competence of the scientist, but arises from the competence of the tribunal. Where evidence of a highly technical nature is involved the court may face difficulties understanding it.⁷²

6.5 Reporting requirements

Malta, the Netherlands and Sweden have no regulation concerning the requirements for statements or reports. Legal regulation does exist in e.g. Austria, Germany, Poland, Portugal, Russia, Slovakia and Spain.

The quality of the expert is of great importance in establishing the value of a statement or findings. However, in France and Portugal, the court does not enquire about the expert's qualifications.⁷³ In England and Wales, experts appear as representatives of the parties. In the remaining European countries court-appointed experts are the norm.⁷⁴

6.6 Admissibility standards

As invited guests of the court, forensic scientists must understand the specifics of their role. Although each country, state and local jurisdiction has its own set of rules governing the acceptance and conduct of expert witnesses, generally, they are quite similar. In the United States, many regulations are – at least to some extent – based on the Federal Rules of Evidence.⁷⁵ Although the specifics vary, a resemblance is that the expert witness, as opposed

⁷² An additional problem in case criminal experts give evidence to a criminal court in England arises from the way that it is presented to the tribunal of fact. Whether this is composed of jurors or lay magistrates, they see no written report in advance, and are expected to absorb the information the expert is called upon to provide through his oral presentation in the witness-box. This is very different from what happens in France and The Netherlands where the expert's report is included in the dossier and the judges will have the chance to read it and to ponder upon it in advance of the trial. In France however, when a case is tried before a jury, the same method as in England applies, giving rise to similar difficulties.

⁷³ L. VAN DER WESTEN, "Organisation and regulation on expert evidence" in J. F. NIJBOER and W. ISPRANGERS (eds.), *Harmonisation in forensic expertise, an inquiry into the desirability of and opportunities for international standards*, Series criminal sciences, Amsterdam, Thela Thesis, 2000, 454.

⁷⁴ H. NIJBOER, "Expert evidence", in R. BULL and D. CARSON (eds), *Handbook of Psychology in legal contexts*, Chichester, John Wiley, 1995, 561.

⁷⁵ Article VII of the United States Federal Rules of Evidence: Opinions and expert testimony.

Rule 703. Basis of opinion testimony by experts: "The facts or data in the particular case upon which an expert bases an opinion or inference may be those perceived by or made known to him at or before the hearing. If of a type reasonably relied upon by experts in the particular field in forming opinions or inferences upon the subject, the facts or data need not be admissible in evidence."

Rule 704. Opinion on ultimate issue. "Testimony in the form of an opinion or inference otherwise admissible is not objectionable because it embraces an ultimate issue to be decided by the trier of fact."

In addition, Rule 403 permits the trial judge to exclude evidence if it would be unduly misleading, confusing or time-consuming. This provides a useful means of keeping away from a jury, material which is not capable of adequate comprehension or resolution as between different versions by a lay tribunal.

to the lay witness, is allowed to give an opinion testimony. Furthermore, they are allowed to explain their answers.⁷⁶

One of the most important roles the analyst must play is that of educator. You can perform the most brilliant analysis, and write the most articulate reports, but if the attorney examining you has not got a clue of what to ask, the whole effort may turn out to be futile. Unfortunately, quality time with the attorney is the first thing to go in the crunch of preparing for trial.⁷⁷

A judge or juror should only base a decision on expert evidence when he or she has good reasons for believing in the validity and reliability of the evidence. Simply trusting the expert just because he is presented as the expert does not constitute a good reason for reliance. The trier of fact (as well as the other parties) must be able to evaluate the evidence critically. The education paradigm might be important⁷⁸, but exclusionary rules of evidence can also play a role. Rules such as the Frye/Daubert rules, employed in the United States, provide a means of keeping unreliable expert evidence out of the courts. Such rules can also articulate the standards to be expected of forensic science techniques. In the absence of exclusionary rules, there are other means by which judges can indicate that certain standards are to be expected of the forensic science evidence presented to them.⁷⁹

6.6.1 Frye⁸⁰

Until the Supreme Court issued its opinion in Daubert, the trial courts determined the admissibility of scientific evidence by applying the ‘general acceptance’ test. This standard was first articulated by the Court of Appeal of the District of Columbia in *Frye v. United States* (1923) which held that expert opinion based on a scientific technique was inadmissible unless the technique was generally accepted in the relevant scientific community as being reliable. In *Daubert*, the Supreme Court held that this “rigid” requirement had been superseded by Rule 702 of the Federal Rules of Evidence.

⁷⁶ K. INMAN and N. RUDIN, *Principles and practice of criminalistics, the profession of forensic science*, A volume in the Protocols in Forensic Science Series, Boca Raton, CRC Press LLC, 2000, 287.

⁷⁷ In one DNA admissibility hearing, the scientist’s failure to educate the prosecution team was in large part responsible for a rejection of the motion. The analyst simply couldn’t be bothered to sit down with the prosecution team and instruct them in the particular procedures he had used and explain potential vulnerabilities they might face in their bid to introduce the testing at trial. The attorneys, working under the mistaken impression that DNA was a shoo-in, were not ready for an exceptionally aggressive and well-prepared defence team.

⁷⁸ What tools might be used to improve the quality of expert evidence? One possibility is that experts should play a more educational role in court, and should not expect judges and jurors simply to defer to their opinions. M. REDMAYNE, “Quality and forensic science evidence: an overview”, in J. F. NIJBOER and W. SPRANGERS (eds.), *Harmonisation in forensic expertise, an inquiry into the desirability of and opportunities for international standards*, Series criminal sciences, Amsterdam, Thela Thesis, 2000, 310 – 313.

⁷⁹ M. REDMAYNE, “Quality and forensic science evidence: an overview”, in J. F. NIJBOER and W. SPRANGERS (eds.), *Harmonisation in forensic expertise, an inquiry into the desirability of and opportunities for international standards*, Series criminal sciences, Amsterdam, Thela Thesis, 2000, 312 – 313.

⁸⁰ The Frye rule (*Frye v. United States*, 293 F. 1013 (1923)), still applied by some state courts, demands that scientific techniques be ‘generally accepted’ before they can be admitted in court, in other words: it rejects scientific evidence unless it is of a type which is generally accepted as valid by professional opinion. [“When exactly does a principle cross the line between experimental and the demonstrable stages? This is difficult to define. Somewhere in this twilight zone, the evidential force of the principle must be recognised, and while the courts will go a long way in admitting expert testimony deduced from a well recognised scientific principle or discovery, the thing from which the deduction is made must be sufficiently established to have gained general acceptance in the particular field in which it belongs.”]

Future of Identity in the Information Society (No. 507512)

Over the years this test provoked a lot of controversy, mainly on the ground that it deprived the courts of the latest advances of scientific knowledge. Moreover, it was said to be unduly difficult to establish what constitutes ‘general acceptance’ within the scientific community, what the relevant scientific community should be regarded as being at any one time and how one determines the scientific character of a theory or technique in the first place. A first attempt to depart from the theory was undertaken in 1978 in the case the United States v. Williams.⁸¹

But soon after, the essentially conservative standard of the Frye test was re-established. During the 1980s, United States courts strove to resolve some of the uncertainty surrounding the implementation of the Frye test. In 1984 it was stressed that the Frye test only applied to novel scientific techniques and methodologies. The party offering the novel scientific evidence has the burden of demonstrating that it has been accepted as reliable among impartial and disinterested experts within the scientific community.

6.6.2 Daubert⁸²

In 1993, the Supreme Court of the United States finally rejected the whole Frye theory in *Daubert v. Merrell Dow Pharmaceuticals, Inc.* laying down more complex criteria for admissibility, including the demonstration of the reliability and validity of techniques, the consideration of their error rates, their logic and the demonstration of professional peer acceptance of new methods. Such scrutiny can have a beneficial effect on the quality of information provided to the courts.⁸³

6.6.3 Kumho

More recently, in *Kumho Tire Company. v. Carmichael* (1999), the U.S Supreme Court expanded the Daubert standard to all sorts of expert testimony, not just strictly ‘scientific’ testimony.⁸⁴ Perhaps anticipating the problems that would follow if any particular Daubert factor was rigidly applied, the Supreme Court emphasised the flexibility that was inherent in the analysis: “We can neither rule out, nor rule in, for all cases and for all time, the applicability of the factors mentioned in Daubert, nor can we now do so for subsets of cases categorised by category of expert or by kind of evidence. Too much depends upon the particular circumstances of the particular case at issue. A flexible approach does not, however, imply a loose one. Even if testimony is based upon professional studies or personal

⁸¹ The court asserted that “The established considerations applicable to admissibility of evidence come into play and the probativeness, materiality and reliability of the evidence on the one side, and any tendency to mislead, prejudice, or confuse the jury on the other, must be the focal points of the inquiry.” The court identified 5 indicators of reliability: 1) potential rate of error in use of the technique; 2) existence and maintenance of standards among its users; 3) care with which the technique was employed in the case; 4) analogy of the technique to others whose results are admissible; and 5) presence of safeguards in the characteristics of the technique.

⁸² In *Daubert*, the Supreme Court created a gate keeping role for trial judges as to the admissibility of scientific expert testimony. The Supreme Court envisioned that trial courts would conduct a factor based analysis when determining whether the testimony was reliable: (1) “whether the theory of technique can be and has been tested” (2) “whether the theory or technique has been subjected to peer review and publication” (3) “the known or potential rate of error” (4) “the existence and maintenance of standards controlling the technique’s operation” and, finally, (5) “‘general acceptance’ can yet have a bearing on the inquiry.”

⁸³ T. GRISSO, *Evaluating competences, forensic assessments and instruments*, New York, Kluwer Academic/Plenum Publishers, 2003, 482.

⁸⁴ K. INMAN and N. RUDIN, *Principles and practice of criminalistics, the profession of forensic science*, A volume in the Protocols in Forensic Science Series, Boca Raton, CRC Press LLC, 2000, 292.

Future of Identity in the Information Society (No. 507512)

experience, trial courts are to ensure that the expert employs in the courtroom the same intellectual rigor that categorises the practice of an expert in the relevant field.”

In *Kumho Tire*, the Supreme Court reaffirmed that trial courts enjoy a certain amount of latitude in their admissibility decisions. A trial court’s decision on whether or not to include expert testimony needs to be reviewed under the abuse of discretion standard.

6.6.4 Other standards

Other scientific evidence standards are the following:

Relevancy test (Federal Rules of Evidence 401, 402, 403): this is embodied in the Federal Rules of Evidence allowing anything that materially assists the trier of fact if it is deemed relevant.

Coppolino standard (*Coppolino v. State*, 1968): the court allows a novel test or piece of new, sometimes controversial, science on a particular problem at hand if an adequate foundation can be laid even if the profession as a whole is not familiar with it.

Marx standard (*People v. Marx*, 1975): the court is satisfied that it did not have to sacrifice its common sense in understanding and evaluating the scientific expertise put before it. This is a ‘common sense’ or ‘no scientific jargon’ test.

6.7 Sanctions on evidence

The principle is that evidence must be rejected if it is illegally or irregularly obtained.

In the United Kingdom, after a long period where rejection was not allowed (“even when you have stolen the evidence, that evidence is still admissible” said a judge in 1861) the exclusion of evidence is allowed in serious situations. Nowadays, evidence may be rejected if it appears that to accept it would have a prejudicial effect on the equity of the trial which in effect gives discretion to the court.

The United States law admits nullity in case of an investigation carried out in contravention of constitutional rights by includes two important restrictions. First of all, illegally acquired evidence may be used if the person against whom the illegality has taken place is not the accused because the latter is not entitled to question the rights of a third party. Additionally, if the illegally obtained evidence would have been discovered in any case, that evidence will be admissible.

In Canada, although in principle the irregularity of evidence is of little importance, the case is different if the evidence has been obtained in violation of a constitutional provision of in violation of the charter and if the use of such evidence ‘might reflect badly on the administration of justice’ (art. 24-2). This concept allows the judge to consider the equity of the trial, the gravity of the violation and also the fact that excluding evidence – even if irregularly obtained – may do more harm to justice than to allow it to be used. This of course supposes a very serious crime and virtually certain guilt based on questionable evidence.

In France nullity is possible in only two cases: if the violation is contrary to the rule of public order (such as competence), or if it is to the detriment of the accused (art. 802 CPP).

The same applies to Switzerland, where one distinguishes irregularity (which has no consequences because the formality which has been violated could have been fulfilled) and illegality, which brings in its wake the rejection of the evidence.

Belgium follows the same line. The matter is dealt with almost exclusively by case law. These cases tend to disapprove procedures where the evidence has been obtained through an

Future of Identity in the Information Society (No. 507512)

illegality or by ignoring the rules of administration. An important cause of nullity is the violation of the rights of the defence or of general principles of procedure, even if the subject has consented.

In Italy the law is stricter. The authors of the code of 1989 used a different notion of nullity, that of non-admissibility (art. 191). The authors stressed the regularity of the procedure whatever the price. Thus any irregularity may bring about the rejection of evidence and such an irregularity can even be a case for rejecting the verdict altogether. With the help of the dossier the judge who is dealing with facts will be aware of illegal evidence but he is not able to make use of it and the possibility for a superior judge to control the reasons of his decision is a way of respecting this principle of non-admissibility.

The Supreme Court of Japan, whilst it lays down the principle of exclusion of illegally obtained evidence, endeavours not to annul procedures especially where the illegality is not serious.⁸⁵

Sometimes the irregularity of the evidence will also apply to derived evidence. If subsequent evidence is linked to the original evidence, then both pieces of evidence must be rejected. This is the theory of 'the fruits of the poisonous tree', an American expression and a concept which is accepted in the US, England, the Netherlands, France but not in Germany.⁸⁶

6.8 Digital evidence

Traditionally, criminal procedure has been oriented towards two sources of information: human beings and tangible objects (items bearing fingerprints, books, blood, etc.). Information technology has added a third one: electronic data. Computer forensics is the detailed examination of computers and their peripheral devices, using computer investigation and analysis techniques in the interests of determining potential legal evidence.

With regard to data stored on external storage media like floppy disks, tapes or CDs, there are no special difficulties because, for procedural purposes, the data can be identified with the object carrying the data.⁸⁷ The only problem left then is the question of how to 'read' the data from the object. However, if data is stored and processed in large and open computer networks, the link with tangible objects gets very loose. The question arises whether data, as distinct from an object, can be made subject to actions under criminal procedure. Can one seize data without the object that it is stored upon for the seizure of the object might be disproportionate or simply technically impossible? Can traditional search powers be used in order to search the data in computers? And, on what legal basis can the data be used in evidence?⁸⁸

⁸⁵ J. PRADEL, "Criminal evidence" in J. F. NIJBOER and W. SPRANGERS (eds.), *Harmonisation in forensic expertise, an inquiry into the desirability of and opportunities for international standards*, Series criminal sciences, Amsterdam, Thela Thesis, 2000, 426 – 427.

⁸⁶ J. PRADEL, "Criminal evidence" in J. F. NIJBOER and W. SPRANGERS (eds.), *Harmonisation in forensic expertise, an inquiry into the desirability of and opportunities for international standards*, Series criminal sciences, Amsterdam, Thela Thesis, 2000, 427.

⁸⁷ Disk forensics consists of making an exact copy of a hard-disk and then analysing it to the point where all manner of apparently hidden and deleted material is made manifest and where it is possible to produce detailed reconstructions of past activity.

Network forensics is about reliability capturing activity on a network, matching it against what might be found on various individual computers and as a result being able to reconstruct activities and actions.

⁸⁸ H. HENSELER and J. ROORDING, "Information technology, the development and regulation of new forensic investigative methods", in J. F. NIJBOER and W. SPRANGERS (eds.), *Harmonisation in forensic*

The term digital evidence encompasses any and all digital data that can establish that a crime has been committed or that can provide a link between a crime and its victim or a crime and its perpetrator.⁸⁹ Digital data is essentially a combination of numbers that represent information of various kinds, including text, images, audio and video. Deleting a file or document by sending it to the recycle bin or trash merely sends it to another part of the computer hard drive. Even when the recycle bin or trash subdirectory is emptied, the file or document is often maintained in a compressed form on the computer's hard drive, and thus is recoverable. That process may well require the expertise of a specialised laboratory or research centre, using uncommon software, but it is no longer impossible.⁹⁰ With the increasing use of computers, digital evidence is becoming more common and more important to investigative efforts. Sometimes information stored on a computer is the only clue in an investigation.⁹¹

6.9 Cybercrime

Crime investigations are increasingly faced with evidence in computers, storage media, telecommunication and data communication. The deductions from traces of these types of evidence are traditionally based on forensic science. The electronic trail can serve as powerful legal evidence against a suspected criminal, as it reveals highly probative 'digital fingerprints' that can potentially be used to prove civil wrongs or criminal activity in a court of law. Searching and finding evidence in digital information requires a new forensic science and new laws. In addition to technical measures, new legislation is required to regulate the application of new investigative methods and the gathering evidence.

The international review of criminal policy⁹² – United States manual on the prevention and control of computer-related crime – categorises 5 common types of computer crime:

- Fraud by computer manipulation
- Computer forgery
- Damage to or modification of computer data or programs
- Unauthorised access to computer systems and service
- Unauthorised reproduction of legally protected computer programs

expertise, an inquiry into the desirability of and opportunities for international standards, Series criminal sciences, Amsterdam, Thela Thesis, 2000, 245.

⁸⁹ This definition is adapted from the definition of physical evidence in R. SAFERSTEIN, *Criminalistics: An introduction to forensic science*, 6th edition, Upper Saddle River, NJ: Prentice Hall, 1998.

⁹⁰ To wipe out some of the compressed information, you would have to reformat the hard drive. However, this is time consuming and does not wipe out all data. The only way to completely wipe out all information is to totally destroy the computer. And even then, the e-mail messages still could be stored in any or all the network servers or Internet service providers (ISPs) used to send or receive that e-mail.

⁹¹ In one case, e-mail messages were the only investigative link between a murderer and his victim. In October 1996, a Maryland woman told her husband she was leaving to visit friends. However, she left a chilling note that caused the husband to inform police about her disappearance. During their investigation, the police found hundreds of e-mail messages between the woman and her lover about their torture and death fantasies. The contents of the e-mail led investigators to the lover's house and they found the grave of the woman nearby. Her hands and feet had been tied and she had been strangled. The lover pleaded guilty, claiming that he killed her accidentally during sex.

⁹² United Nations Crime Prevention and Criminal Justice Programme, *International Review of criminal policy* – United Nations Manual on the prevention and control of computer-related crime, <http://www.ifs.inivie.ac.at/~pr2gg1/rev4344.html>.

Other examples of crime involving the use of computer, such as child pornography on the Internet, money-laundering, illegal gambling on the Internet, credit card fraud and others, should not be viewed as computer crime but as digital equivalents of the ‘real world’ counterparts. Traditional laws apply to these crimes but, nevertheless, new investigation and evidence gathering (i.e. forensics) techniques are required to investigate these matters.⁹³

Many cybercrimes can be addressed using existing laws; after all, cybercrime is just a new manifestation of age-old crimes with the only difference that new technology is employed. However, lawmakers perceived the need for separate statutes to deal with certain forms of computer abuse unambiguously. Many cybercrimes are international in nature and the problems of international co-operation are acute.

6.9.1 EU: Convention on cybercrime (Council of Europe)

The Convention on Cybercrime of 23 November 2001 states the necessity of collecting electronic data for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data in the preamble as well as in several of its articles.⁹⁴ The Convention constitutes the first internationally binding legal instrument with regard to the consequences of modern Information Technology for criminal law and criminal procedure. Notwithstanding that the Council of Europe is a regional body, the Convention provides for a global framework for law enforcement in ‘Cyber-space’, because even non-member states of the Council of Europe such as Canada, Japan and the United States contributed to the preparation of the convention and accordingly signed and supported the agreement.⁹⁵

The Treaty aims to provide harmonised definitions of various computer-related crimes, so that mutual co-operations and extradition can be expedited. Most jurisdictions require some equivalence between their own law and that of the country requesting assistance before they will grant it.

The Treaty also extends towards issues involving evidence, both in terms of warranting methods and actual procedures. With regard to electronic evidence, Recommendation No R(95) 13 of the Committee of Ministers of the Council of Europe concerning problems of

⁹³ H. HENSELER and J. ROORDING, “Information technology, the development and regulation of new forensic investigative methods”, in J. F. NIJBOER and W. SPRANGERS (eds.), *Harmonisation in forensic expertise, an inquiry into the desirability of and opportunities for international standards*, Series criminal sciences, Amsterdam, Thela Thesis, 2000, 234 – 236.

⁹⁴ Council of Europe, Convention on Cybercrime of 23 November 2001, <http://conventions.coe.int/Treaty/en/Treaties.Html/185.htm>.

Preamble:

- Concerned at the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

- Taking into account the existing Council of Europe conventions on co-operation in the penal field as well as similar treaties which exist between Council of Europe member States and other States and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

⁹⁵ Chart of signatures and ratification of the Convention on Cybercrime: <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=09/07/04&CL=ENG> The Convention on Cybercrime entered into force on 1 July 2004.

Future of Identity in the Information Society (No. 507512)

criminal procedural law connected with information technology⁹⁶, adopted on 11 September 1995, states the following (principle IV.13):

“Special procedures and technical methods for handling electronic evidence should be developed which ensure and reflect the integrity and authenticity of the evidence. Legal provisions on evidence relating to traditional (paper) documents should similarly apply to electronic documents.”

The Explanatory Memorandum to the Recommendation explains the difficulties of electronic evidence as opposed to paper documents (par. 152f of the Explanatory Memorandum): “Among other things electronic documents can only be read by means of special hard and software and they can be easily manipulated in such a way that the manipulation is not detectable by the eye.” The Explanatory Memorandum suggests different procedures for authentication of electronic evidence, like the establishment of a complete chain of custody – from the person who first copied the data to the person who produced the printout for the trial – or the use of electronic signatures (par. 161). The development of a harmonised approach in this matter at an international level is indispensable because information technology offences are often characterised by a cross-border nature (par. 164). Otherwise, according to the Explanatory Memorandum, serious problems with regard to the admissibility of electronic evidence will continue to exist.

The Treaty in its current form does not appear to address problems of disclosure of evidence to the defence. In most countries, defence lawyers are entitled to see all the evidence of their client. In the UK, the prosecution is under the constant duty to disclose to the jury anything which might undermine the prosecution case; after receiving a defence case statement, the prosecution also has to consider what might reasonably assist the defence.⁹⁷ Problems will occur when the evidence was collected by an overseas law enforcement agency that feels that their obligations cease at their own borders.⁹⁸

6.9.2 The Netherlands: the Computer Crime Act of 1993

The Computer Crime Act of 1993⁹⁹ has not changed the Dutch law of evidence. There was no need for such adaptation because the country’s law of evidence is rather flexible. The law provides for some broad categories of evidence, like the official report of a police officer containing his observations, and the personal observations by the Court. Furthermore, the conviction of the Court is decisive whether or not the case has been proven. Therefore, computer evidence – printouts of intercepted e-mails, data gathered in computers and stored on tape or floppy disk – does not cause any difficulties.¹⁰⁰

⁹⁶ Recommendation No R (95) 13 of the Committee of Ministers of the Council of Europe concerning problems of criminal procedural law connected with information technology, adopted on 11 September 1995, <http://www.coe.fr/cm/ta/rec/1995/95r13.htm>.

⁹⁷ Criminal Procedures and Investigations Act, 1966, plus Codes of Practice and Attorney-General’s Guidelines. <http://www.lso.gov.uk/pdf/guidelines.pdf>.

⁹⁸ P. SOMMER, *Emerging problems in digital evidence*, UKCLE/LTSN-ICS Law Crime and the Internet Conference, University of Warwick, 17 March 2004.

⁹⁹ Official Journal of The Netherlands (Staatsblad) 1993, nr. 33.

¹⁰⁰ H. HENSELER and J. ROORDING, “Information technology, the development and regulation of new forensic investigative methods”, in J. F. NIJBOER and W. SPRANGERS (eds.), *Harmonisation in forensic expertise, an inquiry into the desirability of and opportunities for international standards*, Series criminal sciences, Amsterdam, Thela Thesis, 2000, 249.

6.9.3 Belgium: Computer Crime Act of 2001

Since November 2001, Belgium has its very own law on cybercrime.¹⁰¹ Before, only moveable objects could be seized, consequently the seizure of electronic data was only possible through seizure of the material carrier of the data, like a disk or a computer. The Cybercrime Act introduces a new article 39b in the Code of Criminal Proceedings, which provides a means of coercion with the same objectives as seizure. When the examining magistrate comes across useful data in an informatics system, he is allowed to copy the data without being forced to seize the material carrier.

6.9.4 United States: Computer Fraud and Abuse Act (CFAA) and the Electronic Communications and Privacy Act (ECPA)

The CFAA was enacted in 1984 and has been amended several times since. Practically all states have additional computer crime statutes that extend the CFAA.

Investigators sometimes need to obtain the destination, origin or even the content of certain communications. Since all this information is normally considered private, certain procedures have been put in place to prevent anyone, particularly the government, from misusing this information. The Fourth Amendment requires that a search warrant be secured before law enforcement officers can search a person's house, person, papers and effects.¹⁰² As computer networks became more widely used, lawmakers deemed it necessary to introduce more stringent privacy laws to protect information that is stored on and transmitted through computers specifically. To this end, the ECPA was enacted in 1986 to protect all forms of electronic communications. The law stipulates that, to obtain authorisation to intercept transmissions, law enforcement must follow a specific procedure and obtain a court order (or another certification in writing) that satisfies a given list of requirements. These rigid requirements make it more difficult to obtain authorisation to intercept electronic transmissions. There is more flexibility when it comes to stored electronic communications. The distinction between the two was made because intercepting transmissions potentially entails a greater invasion of privacy than collecting stored communications.¹⁰³

By obtaining consent to search, investigators can perform a search without a warrant.¹⁰⁴

¹⁰¹ Law of 28 November 2001 concerning informatics crime, *Official State Gazette* 3 February 2002, 2909 – 2914.

¹⁰² The ECPA prohibits anyone, not just the government, from unlawfully accessing or intercepting electronic communications, whereas the Fourth Amendment only applies to the government.

¹⁰³ When intercepting communications, there is a high chance that unrelated, private information will also be intercepted whereas stored communications are more discrete and the chance of collecting unrelated, private information is limited. E. CASEY, *Digital evidence and computer crime, forensic science, computers and the Internet*, London – San Diego, Academic Press, 2000, 207 – 222.

¹⁰⁴ A consent form should be used when obtaining consent to reduce the chance of the search being successfully challenged in court. A warrantless search can be made for any emergency threatening life and limb. It is difficult to imagine a case in which a computer could be collected under exigent circumstances. Even in a homicide, a warrant is required for an in-dept search of the suspect's possessions.

6.10 Electronic signatures¹⁰⁵

6.10.1 European Union

Within the European Union, the Electronic Signature Directive from 13 December 1999 has contributed to the value of electronic signatures.¹⁰⁶ In the past, only hand-written signatures were legally valid, but the new legislation extends that recognition to electronic signatures and applies the Internal Market principles of free movement of services and home country control to e-commerce. In doing so, it constitutes an important element in the Commission's ongoing efforts to drive forward the rapid development of electronic commerce.

The Directive defines an electronic signature as: "Data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication."¹⁰⁷

As to the legal effects of electronic signatures¹⁰⁸, article 5 of the Directive states the following:

"1. Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device: (a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and (b) are admissible as evidence in legal proceedings.

2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:

- in electronic form, or

¹⁰⁵ For extensive reading I refer to the Doctoral Thesis of P. VAN EECKE concerning the electronic signature, *Naar een juridische status voor de elektronische handtekening, een rol voor de handtekening in de informatiemaatschappij?* Proefschrift tot verwerving van de graad van doctor in de rechten, K.U. Leuven, 2004.

¹⁰⁶ Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, *O.J. L 13/12*, 19 January 2000.

¹⁰⁷ Article 2, 1 of Directive 1999/93/EC on electronic signatures, *ut supra*. Article 2, 2: "An advanced electronic signature means an electronic signature which meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using means that the signatory can maintain under his sole control; and (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable."

¹⁰⁸ Recital 16: "This Directive contributes to the use and legal recognition of electronic signatures within the Community; (...) the legal effectiveness of electronic signatures (...) and their admissibility as evidence in legal proceedings should be recognised."

Recital 20: "Harmonised criteria relating to the legal effects of electronic signatures will preserve a coherent legal framework across the Community; national law lays down different requirements for the legal validity of handwritten signatures; whereas certificates can be used to confirm the identity of a person signing electronically; advanced electronic signatures based on qualified certificates aim at a higher level of security; advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device can be regarded as legally equivalent to handwritten signatures only if the requirements for handwritten signatures are fulfilled."

Recital 21: "In order to contribute to the general acceptance of electronic authentication methods it has to be ensured that electronic signatures can be used as evidence in legal proceedings in all Member States; the legal recognition of electronic signatures should be based upon objective criteria and not be linked to authorisation of the certification-service-provider involved; national law governs the legal spheres in which electronic documents and electronic signatures may be used; this Directive is without prejudice to the power of a national court to make a ruling regarding conformity with the requirements of this Directive and does not affect national rules regarding the unfettered judicial consideration of evidence."

Future of Identity in the Information Society (No. 507512)

- not based upon a qualified certificate, or
- not based upon a qualified certificate issued by an accredited certification-service-provider, or
- not created by a secure signature-creation device.”

6.10.2 United States

In the United States, the Congressional Bill of 30 June 2000 gives electronic signatures the same force and effect as pen-and-ink signatures. The law was not revolutionary at all since the majority of states has already recognised some forms of electronic signatures before Congress stepped up to the plate.

6.11 Impediments of digital evidence

Everywhere in the world, the ability of government investigators to search for evidence is limited by the reasonable expectation of privacy. This restricts law enforcement from investigating a person’s private computer files without probable cause and a warrant.¹⁰⁹ When probable cause is proven absent, the evidence obtained is suppressed under the exclusionary rule. Therefore, searchers must first obtain a valid search warrant based on probable cause to ‘search’ – which really translates to ‘analyse’ – personal technological devices and electronic data for evidence of a crime or criminal activity.

Question remains when exactly the privacy comes into play. The potential for confusion regarding the expectation of privacy is extremely high.

The presence of computers has created additional complexities and definitional problems within the accepted rules of evidentiary procedure. To a large degree, these difficulties are a direct result of the very qualities inherent in digital data. The ease with which electronic impulses can be manipulated, modified, and erased is hostile to a legal system that arose in an era of tangible things and relies on documentary evidence to validate transactions and prove contractual relations.

The credibility of digital evidence has been thoroughly debated in literature. One magazine for example once predicted the end of photography as evidence of anything.¹¹⁰ Another author wrote that a picture could tell a thousand lies.¹¹¹ Many photographers use digital imaging technology specially because of its manipulability; everyday examples include a commercial photographer removing unwanted elements from an advertisement or even NASA scientists enhancing images transmitted from satellites.

Alterations can occur in one of the three following contexts: it may be accidental, intentional but innocent, or fraudulent. Accidental alteration might result from a variety of causes, for example, a magnetic disk on which data is stored might be placed too close to a powerful

¹⁰⁹ In the USA, the courts apply the Fourth Amendment to electronic information as they do to any other form of evidence.

¹¹⁰ S. BRAND et al., “Digital Retouching: the End of Photography as Evidence of Anything”, *Whole Earth Review*, July 1985.

¹¹¹ C. GUILSHAN, “A Picture is Worth a Thousand Lies: Electronic Imaging and the Future of the Admissibility of Photographs Into Evidence”, 18 *Rutgers Comp. & Technology. Law Journal* 365, 374 – 75 (1992).

Future of Identity in the Information Society (No. 507512)

magnetic field – such as that generated by some computer monitors.¹¹² The effects of accidental alteration are likely to be catastrophic, and it is difficult to imagine what evidentiary problems could follow beyond those commonly raised by destroyed documents. If, on the other hand, someone intentionally manipulated an image for fraudulent purposes, there's no easy method of detection.¹¹³

Technology can create problems, but it can also be employed to solve problems. Although digital data possesses qualities that give rise to evidentiary concerns, it also possesses qualities that can be applied to meet those concerns. A technical response might, for instance, build upon one last characteristic feature of digital data: it can include, as an integral part, data about itself. It is possible to attach a 'digital signature' to a file, encrypted to prevent alteration, verifying that the data has not changed since the attachment was generated. This verification extends to cover perfect digital copies (including the attachment) but belies an altered file, whether it is a copy or the original.

With the ever-increasing use of computers over the last decade, the use of Computer Forensic Specialists will become more and more important. It is imperative that the legal and professional fraternities know and understand the ramifications of not using properly qualified experts.

The most important aspect is that the Computer Expert will present the information in a manner that is recognised by the court system and will be able to explain the facts in an easy to understand manner.

6.12 Admissibility of digital evidence in court

Perhaps as a result of the abovementioned difficulties, courts have been slow to construct doctrines governing the admissibility of digital evidence. In only a few decades, computers have evolved from imaginary science fiction into equipment of our daily lives. As a social institution, the judicial system will have to adapt to the influence of computers if it is to remain responsive in the years ahead.

It is up to the court to decide whether the evidence will be accepted in court or not. This is especially true when dealing with computerised data of which the production can represent a substantial expense. If the party requiring the research in question is unable to convince the court of the relevance of the evidence, it can be overruled.¹¹⁴ The court can also appoint an expert for electronic discovery whenever it deems this a necessary step towards revealing the truth.¹¹⁵

¹¹² Warnings against this danger are typically found on the boxes in which computer disks are purchased, usually in the form of an indecipherable pictogram.

¹¹³ R. McCARVEL, "You won't believe your eyes: digital photography as legal evidence", 1995, <http://www.seanet.com/~rod/digiphot.html#III1>.

¹¹⁴ *Fennell v. First Step Design, Ltd.*, 83 F.3d 526 (1st Cir. 1996) The plaintiff's electronic discovery request was denied by the court, as the plaintiff didn't establish a 'particularized likelihood of discovering appropriate information.'; *Lawyers Title Ins. Co. v. U.S.F. & G.*, 122 F.R.D. 567 (N.D.Cal. 1988) The electronic discovery was not allowed unless shown that it would lead to material that wasn't previously produced; *Strausser v. Yalamachi*, 669 So.2d 1142, 1144-45 (Fla. App. 1996) The discovery request was denied. The court determined the likelihood of recovering information very small. Furthermore, the system contained confidential patient records. The appeals court ruled that the request was inordinate.

¹¹⁵ *Playbody Enterprises, inc. v. Terry Welles*, 60 F. Supp 2 1050; 1999 U.S. Dist. LEXIS 12895 (S.D. Cal. 1999) The court can appoint a neutral expert to recover deleted email; *Simon Property Group v. mySimon, Inc.*, 2000 WL 963035 (S.D. Ind) The court ordered a special master for electronic discovery

Future of Identity in the Information Society (No. 507512)

On the other hand there are a lot of examples of cases whereby one party was sanctioned for failing to preserve the requested electronic evidence.¹¹⁶

A big concern is the clash between the need to recognise that certain types of information are regarded as privileged and the need to preserve the integrity of computer evidence by means of imaging. Communications between a lawyer and his client is one example of privilege. In the United Kingdom, the case of *R. v. Chesterfield Justices and Chief Constable of Derbyshire ex parte Bramley* (CA, 1999) brought these issues in the open. In that particular case, documents of a car dealer, which included correspondence with his solicitor, were seized from his premises. While the court recognised the common sense arguments in favour of seizing a mass of material and then sorting it out elsewhere, it was forced to conclude that any seizure later found to be outside the scope of the warrant could expose the police to a successful action for trespass of goods. An attempt has been made to address this problem in Part 2 of the Criminal Justice and Police Act, 2001 and associated Codes of Practice. Section 54 restates the rule that legally privileged material seized in a warrant must be returned. But it goes on to say that legally privileged material can be retained if it is ‘inextricably linked’ to other material which is seizable.¹¹⁷

Another concern is the distinction between ‘communications data’ (who called whom, when and for how long) and the ‘content’ of a conversation (what was actually said). In the United Kingdom the former is admissible while the latter is not and cannot be referred to; law enforcement can only use it for intelligence purposes. Most jurisdictions similar to the UK do not make this distinction and the general debate about the value and wisdom of excluding this class of evidence lives on. It could be noted that nowadays it is very difficult to make the separation between communications data and content. In the past, the intercepted call was on an analogue telephone which enabled the separation of the two. However this separation simply does not exist for most Internet-based forms of communication. Communication data and content are digital and the most convenient technical means to capture ‘communications data’ is often identical to that for capturing ‘content’.¹¹⁸¹¹⁹

Obviously there are some requirements the electronic production has to meet. For example, the court demands material to be produced in a ‘reasonably usable form’.¹²⁰ Section 19 of the Police and Criminal Evidence Act from 1984 (UK) allows the constable to require that information held in a computer “be produced in a form in which it can be taken away and in which it is visible and legible.”

¹¹⁶ *Computer Associates International v. American Fundware, Inc.*, 133 F.R.D. (D. Colo. 1990); *Lauren Corp v. Century Geophysical Corp.*, 1998 Colo. App. LEXIS 12 (No. 96CA0554, Jan. 22, 1998); *Linnen v. A.H. Robins Co. Inc.*, 10 Mass. L. Rptr. 189 (1999); *Prudential Ins. Co. of America Sales Practices Litigation*, 169 F.R.D. 598 (1997); *Shaw v. Hughes Aircraft*, Orange County Superior Court (1996).

¹¹⁷ P. SOMMER, *Emerging problems in digital evidence*, UKCLE/LTSN-ICS Law Crime and the Internet Conference, University of Warwick, 17 March 2004.

¹¹⁸ Are web-requests purely communications data? Or may they include an element of content? What happens at a technical level when you send a request to a web-based search engine or to an e-commerce server? And in e-mails: are the headers to be considered as communications data or content?

¹¹⁹ P. SOMMER, *Emerging problems in digital evidence*, UKCLE/LTSN-ICS Law Crime and the Internet Conference, University of Warwick, 17 March 2004.

¹²⁰ *Greyhound Computer Corp., Inc v. IBM 3 Computer L. Serv. Rep.*, 138, 139 (D. Minn. 1971).

Future of Identity in the Information Society (No. 507512)

However, the printing out of large amounts of data results in the receiving party spending considerable time analysing the information, whereas receiving the data in electronic form would allow the receiving party to conduct the necessary analysis themselves.¹²¹

Section 69 of the Police and Criminal Evidence Act from 1984 deals specifically with the admissibility of evidence from computer records in criminal proceedings. It reads:

“(1) In any proceedings, a statement in a document produced by a computer shall not be admissible as evidence of any fact stated therein unless it is shown

- a. that there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer;
- b. that at all material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the inaccuracy of its contents;(…)”

6.13 Physical evidence

Identification frequently suffices to meet a legal standard of proof. This is evident in crimes that involve illicit substances like drugs, where the mere possession of specified chemicals is deemed illegal. Another example is the assessment of DUI (driving under the influence) where the finding of a particular concentration of alcohol in a person’s blood, breath, or urine, by definition legally prohibits the operation of a motor vehicle. These limited situations are the only times that physical evidence can be considered direct evidence as opposed to circumstantial evidence.¹²²

Criminalists agree that certain categories of evidence inherently contain individualising potential¹²³:

1. Physical match evidence¹²⁴
2. Print and impression evidence
 - a. Tool marks of all kinds, including firearms
 - b. Shoeprints (as opposed to footprints)
 - c. Biological prints including fingerprints, footprints, and those from other body parts, such as ears and lips.

¹²¹ *Minnesota v. Philip Morris Inc.*, No. CI-94-8565 (Dist. Ct. Minn. 1994).

Hard-disk capacities are rising all the time – an ordinary retail PC now routinely features 120 GB hard-disks, as opposed to the 20 GB of only two years ago. Simply in terms of ‘imaging’ and subsequent analysis, law enforcement technicians find their workload multiplying overnight. How does a prosecution serve such a quantity of material on the defence? Printing everything out doesn’t seem like an option.

¹²² K. INMAN and N. RUDIN, *Principles and practice of criminalistics, the profession of forensic science*, A volume in the Protocols in Forensic Science Series, Boca Raton, CRC Press LLC, 2000, 122.

¹²³ K. INMAN and N. RUDIN, *Principles and practice of criminalistics, the profession of forensic science*, A volume in the Protocols in Forensic Science Series, Boca Raton, CRC Press LLC, 2000, 130.

¹²⁴ This constitutes an often ignored but highly useful category of evidence. Probably the first recorded case in which physical matching led to a suspect was that of John Toms in England in 1784. The torn edge of a piece of newspaper used for wadding in his pistol matched a remaining piece in his pocket. Because of the random nature of its generation, physical matching is often perceived as very strong evidence. However, because the analysis of physical match evidence requires no fancy instrumentation or chemical reactions, and the interpretation is based on common sense, cases in which it plays a significant role do not tend to make the history annals. K. INMAN and N. RUDIN, *Principles and practice of criminalistics, the profession of forensic science*, A volume in the Protocols in Forensic Science Series, Boca Raton, CRC Press LLC, 2000, 35.

Future of Identity in the Information Society (No. 507512)

3. Handwriting evidence
4. DNA analysis of biological evidence

Overall, these categories can be classified into two broad groups: non-biological and biological evidence.

6.14 Non-biological evidence

Most common examples in this category are firearms, tool marks, vehicles...

In the case of *Ramirez v. State of Florida*¹²⁵, a decision of the Supreme Court of Florida of 2001, a conviction was reversed because of the erroneous admission of a testimony by a tool mark expert witness who had identified a particular knife as the murder weapon from a microscopic comparison of markings in a piece.

In each of the three successive murder trials preceding the abovementioned decision of the Supreme Court, a police crime technician made the extraordinary claim that his newly formulated knife mark identification procedure was infallible. He contended that he could identify the murder weapon to the exclusion of every other knife in the world – even if there had been two million consecutively produced knives of the same type – based on a striation ‘signature’ arising from microscopic imperfections in the steel of the blade. The trial court in all three trials agreed to the expert testimony and Ramirez was convicted of first-degree murder and subsequently sentenced to death.

The Supreme Court reviewed the case and was convinced that “under the general acceptance test of *Frye*, the State has failed to prove that the testing procedure used to apply the underlying scientific principle to the facts has gained general acceptance in the field in which it belongs. In sum, the expert’s mark identification procedure can, for the time being, not be said to carry the imprimatur of science. The procedure is a classic example of the kind of novel ‘scientific’ evidence that *Frye* was intended to banish, i.e. a subjective, untested, unverifiable identification procedure that purports to be infallible. The potential for error or fabrication in this procedure is inestimable.”

6.15 Biological evidence – biometric identification

Biometrics technology can be used for the purpose of either identification or verification. In general, biometric identifiers can acquire unique biological information from people to verify their identity, much like a pin number for a credit card or a driver’s license function. The most commonly known method of biometric identification is fingerprint biometrics, which is used by police forces throughout the whole world. DNA identification is another popular and increasingly non-controversial use of biometric technology. Other biometrical methods of identification include retinal and iris scans, hand geometry, facial feature recognition, ear shape, body odour, brain fingerprinting, signature dynamics, voice verification, and computer keystroke dynamics to name a few.

These technologies have many potential uses in the criminal justice system: to enhance access control and identity verification in correctional facilities but also as an investigative tool for

¹²⁵ *Joseph Ramirez v. State of Florida*, Supreme Court of Florida, 20 December 2000, WL 1628609, 27 Fla. L. Weekly S18, 2001.

identifying missing and exploited children as well as criminals captured by surveillance systems.¹²⁶

For some types of evidence, the connection to the crime is not necessarily obvious. We each lose hundreds of hairs a day, so the finding of human hair almost anywhere is predictable. The finding of human hairs at a crime scene is therefore to be expected; whether or not the hairs bear any relation to the crime. The presence of hairs that appear to have been forcibly removed immediately suggests increased relevance to the crime; bloody clumps of hair increase that relevance exponentially.¹²⁷

When assessing the legality and reliability of the results of forensic examinations performed in another country, the court should have insight into the forensic method and the circumstances under which the sample was obtained and the analysis performed. Harmonisation of the legal prerequisites for forensic scientific examination within Europe – with the European Convention for Human Rights as the reference point – will make the court’s assessment easier.¹²⁸

6.15.1 DNA profiling (also known as DNA fingerprinting)

“DNA testing is to justice what the telescope is for the stars: not a lesson in biochemistry, not a display of the wonders of magnifying optical glass, but a way to see things as they really are. It is a revelation machine.”¹²⁹

- B. SCHECK -

Article 8¹³⁰ of the European Convention on Human Rights spells out the right to privacy and a privilege against self-incrimination can be derived from article 6¹³¹. According to article 8, the

¹²⁶ A. JARVIS, “Biometric Identification. Facial recognition, retinal iris scans, DNA, fingerprinting, brain printing, ear matching, smart cards... What’s next?”, http://www.forensic-evidence.com/site/ID/ID_Biometric_jarvis.html.

¹²⁷ K. INMAN and N. RUDIN, *Principles and practice of criminalistics, the profession of forensic science*, A volume in the Protocols in Forensic Science Series, Boca Raton, CRC Press LLC, 2000, 105. The case of *People v. Axell* involved the stabbing murder of a convenience store clerk by an unknown female. The victim was found clutching 10 anagen hairs in his fist – anagen hairs are in the growth phase and would not be expected to fall out easily – a circumstance consistent with the victim having pulled the hair from someone’s head during a struggle. Because anagen hairs must be forcibly removed from the scalp, it is reasonable to infer that a clump of hair clutched in the hand of a murder victim is related to the assault that killed him. DNA analysis of the hair led to Linda Axell. While the DNA analysis was vital to increasing the strength of the evidence by virtually individualizing the hairs to Linda Axell, their significance in the context of the crime was determined wholly by circumstance. The hairs were determined to be relevant to the homicide by virtue of their location (his hand) and by their apparent state as pulled hairs. If they weren’t, the results of the DNA analysis would have been less significant in the context of the crime.

¹²⁸ L. VAN DER WESTEN, “Legal regulations governing forensic scientific methods” in J. F. NIJBOER and W. SPRANGERS (eds.), *Harmonisation in forensic expertise, an inquiry into the desirability of and opportunities for international standards*, Series criminal sciences, Amsterdam, Thela Thesis, 2000, 291.

¹²⁹ B. SCHECK, P. NEUFELD and J. DWYER, *Actual innocence: five days to execution and other dispatches from the wrongly convicted*, New York, Doubleday, 2000.

¹³⁰ Article 8 ECHR: “1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

¹³¹ Article 6 ECHR: “1. In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be

Future of Identity in the Information Society (No. 507512)

right to privacy may be limited by a legal regulation that is necessary in a democratic society. Against this background, the DNA legislation of the Member States of the Council of Europe contains a provision concerning the collection of biological evidence from suspects. Moreover the collection of samples and the use of DNA analysis must be in conformity with the Council of Europe's standards of data protection as laid down in the Data Protection Convention No 108 and the Recommendations on data protection, in particular Recommendation (87) 15 regulating the use of personal data in the police sector.

The Recommendation of the Council of Europe dealing with the use of DNA analysis within the framework of the criminal justice system (1992)¹³² states the following: "The taking of samples for the purpose of DNA analysis should only be carried out in circumstances determined by the domestic law; it being understood that in some States this may necessitate specific authorisation from a judicial authority.

Where the domestic law admits that samples may be taken without the consent of the suspect, such sampling should only be carried out if the circumstances of the case warrants such action."

Most countries require the consent of the prosecutorial office or an examining magistrate in order to collect biological evidence from a suspect. In France and Spain, samples may only be taken with the consent of the person in question.¹³³

The Netherlands

Since 1994, DNA profiling is actively used as forensic evidence. The Code of Criminal Proceedings stipulates the conditions for DNA profiling. This law establishes, among others, which authority may order a DNA analysis and under what circumstances a suspect must cooperate. Prescribed practice is laid down in subordinate regulations. These regulations determine, among others, which laboratories may perform a DNA analysis, how samples must be obtained, how the identity of the samples must be ensured and what standards of quality the laboratory must meet. In addition, a separate regulation has been drawn up for the DNA database. The law does not specify the forensic method to be used in DNA profiling.

Taking samples from a suspect without consent for DNA analysis is subject to certain restrictions. Since 1994, the Dutch legislation enables the taking of samples without the suspect's consent if the offence in question is punishable by a prison sentence of 4 years or more or if the offence belongs to a certain category of offences including sexual offences.

excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice. 2. Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law. 3. Everyone charged with a criminal offence has the following minimum rights: a) to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him; b) to have adequate time and facilities for the preparation of his defence; c) to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require; d) to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him; e) to have the free assistance of an interpreter if he cannot understand or speak the language used in court."

¹³² Council of Europe, Recommendation (92) 1, 10 February 1992, on the use of DNA analysis within the framework of the criminal justice system.

¹³³ L. VAN DER WESTEN, "Legal regulations governing forensic scientific methods" in J. F. NIJBOER and W. SPRANGERS (eds.), *Harmonisation in forensic expertise, an inquiry into the desirability of and opportunities for international standards*, Series criminal sciences, Amsterdam, Thela Thesis, 2000, 284.

Future of Identity in the Information Society (No. 507512)

These are the only cases in which an order to take a sample may be given. Of course these conditions do not apply if the suspect consents.¹³⁴

Spain / France

Samples may only be taken with the consent of the person in question.

United States

The introduction of DNA technology into the United States legal system occurred in a Pennsylvania murder case in 1987. The accused funeral director and his wife were charged with the murder of a 92-year old retired coal miner who had been under their protection. An autopsy revealed that the old man had been severely malnourished and that he died from starvation. Nonetheless, the funeral director was granted permission to bury the old man's remains. Some time later suspicions of macabre foul play surfaced and the prosecutor obtained an order for the old man's exhumation and re-autopsy. The prosecutor suspected the funeral director of interfering with the remains so as to confound the real reason for the old man's death. The products used in the embalming process disrupted the blood typing. DNA testing took place but the test failed to support the prosecutor's thesis since the DNA was found to be severely broken.¹³⁵

In *The State of Florida v. Tommie Lee Andrews* (March 1988), the result of conventional testing of semen was inconclusive. A blood group substance was identified but appeared to be that of a substantial proportion of the population. DNA testing was able to establish a pattern that would occur in one of 840 million persons. Two trials of the defendant were held, since the first jury was unable to reach a confirmed verdict.

One year later, in 1989, the admissibility of DNA identification was considered in *The People v. Joseph Castro*, a decision of the Supreme Court of the State of New York. In this case the defendant was accused of murdering a young pregnant girl and her daughter. A wristwatch with bloodstains, worn by the defendant at the time of his arrest, was seized. A DNA identification test matched the bloodstains to the blood of the adult victim.

As from January 1989, the Federal Bureau of Investigation (FBI) began to accept casework from state forensic labs. Since then, DNA fingerprinting has been used in hundreds of cases in the United States and has been formally allowed in at least one jurisdiction in about two-thirds of the states.

United Kingdom

Forensic use of DNA technology in criminal cases began in the United Kingdom in 1986.¹³⁶ DNA profile evidence led to the discharge of a young man who had been held in custody for some months after being charged with the murder and rape of a schoolgirl. The accused was

¹³⁴ Law of 5 July 2001 amending the regulation of DNA investigation in criminal cases, *Official State Journal* 2001, 335.

¹³⁵ I. FRECKELTON, "DNA profiling – a legal perspective" in J. ROBERTSON (ed.), *DNA in forensic science: theory, techniques and applications*, New York, Ellis Horwood series in forensic science, 1990, 168 – 169.

¹³⁶ The first reported use of DNA identification was in a non-criminal setting to prove a familial relationship. A Ghanaian boy was refused entry into the United Kingdom for lack of proof that he was the son of a woman who had the right of settlement in the U.K. Immigration authorities contended that the boy could be the nephew of the woman, not her son. DNA testing showed a high probability of a mother-son relationship. The U.K. Government accepted the test findings and admitted the boy. See K. KELLY, J. RANKIN and R. WINK, "Methods and Applications of DNA Fingerprinting: A Guide for the Non-Scientist," *Criminal Law Review*, 1987, 105 – 108.

Future of Identity in the Information Society (No. 507512)

suspected of having committed a similar crime in 1983. Conventional tests revealed that the same man could have committed both crimes, but the frequency of occurrence of the relevant groups meant that the semen could have come from at least 10% of the male population. DNA profiling was then carried out on a whole blood sample and a bloodstain from the suspect. It conclusively excluded the suspect as the rapist.

In 1987, Colin Pitchfork, a 27-year-old baker in Leicestershire, England, became the first murderer convicted on DNA evidence. Officers investigating the rape and murder of two teenage girls took consensual blood samples from more than 5,000 people throughout three nearby villages. These samples were first screened by standard blood typing to reduce the pool of possible suspects to a size suitable for the costly and time-consuming DNA profiling techniques. Pitchfork's DNA matched the semen recovered from the bodies. Intriguing aspects of the case convinced the UK Home Office and Scotland Yard of the veracity of DNA profiling and led to universal recognition of its potential power.¹³⁷

Other countries

Some other countries (Germany, Poland, and Turkey) also have legal restrictions that limit the possibility of sampling. Once the prosecutorial office or the examining magistrate has authorised sampling, the suspect is in theory compelled to provide a body tissue sample for analysis. Not every suspect is willing to co-operate. Legislation in several countries allows the use of physical force under those circumstances (Austria, Germany, Poland, Turkey, Slovakia, Sweden, The Netherlands). The refusal to co-operate after a justice authority has give authorisation, can also be punished as a separate punishable offence (Slovakia, Turkey, in Germany only if there is a victim).¹³⁸

6.15.1.1 Case law DNA¹³⁹

The abovementioned Recommendation of the Council of Europe dealing with the use of DNA analysis within the framework of the criminal justice system (1992)¹⁴⁰ stresses that "Recourse to DNA analysis should be permissible in all appropriate cases, independent of the degree of seriousness of the offence."

There are quite a few cases in which DNA testing after the trial shed a new light on the available evidence.¹⁴¹ DNA test results represented newly discovered evidence obtained after completion of the trials.¹⁴² Most cases involved some form of sexual assault, for which the defendant was convicted and serving a sentence of incarceration. While in prison, each

¹³⁷ S. EASTEAL, N. McLEOD and K. REED, *DNA profiling, principles, pitfalls and potential*, Chur, Harwood academic publishers, 1991, 4.

¹³⁸ L. VAN DER WESTEN, "Legal regulations governing forensic scientific methods" in J. F. NIJBOER and W. SPRANGERS (eds.), *Harmonisation in forensic expertise, an inquiry into the desirability of and opportunities for international standards*, Series criminal sciences, Amsterdam, Thela Thesis, 2000, 285.

¹³⁹ E. CONNORS, T. LUNDREGAN, N. MILLER and T. McEWEN, US Department of Justice, *Convicted by juries, exonerated by science: Case studies in the use of DNA evidence to establish innocence after trial*, Alexandria, National Institute of Justice, 1996.

¹⁴⁰ Council of Europe, Recommendation (92) 1, 10 February 1992, on the use of DNA analysis within the framework of the criminal justice system.

¹⁴¹ Gilbert Alejandro (1990, Uvalde County, Texas), Kirk Bloodsworth (1985, Baltimore, Maryland), Mark Diaz Bravo (1990, Los Angeles County, California), ...

¹⁴² In the United States, states have time limits on filing motions for new trials on the basis of newly discovered evidence. For example in Virginia, new evidence must be presented by motion within 21 days after the trial. Therefore sometimes a pardon from the governor is required to release the defendants from prison when the given time has elapsed.

Future of Identity in the Information Society (No. 507512)

defendant obtained, through an attorney, case evidence for DNA testing and consented to a comparison of the evidence-derived DNA to his own DNA sample. In some cases, the results showed that there was not a match, and the defendant was consequently set free.

A majority of the cases in question involved non-DNA-tested forensic evidence that was introduced at trial. Typically, those cases involved comparisons of non-victim blood, semen or hair at the crime scene to that of the defendants. Testimony and prosecution experts were also used to explain the reliability and scientific strength of non-DNA evidence to the jury.

Attempts have been made to move toward reducing the incidence of unreliable evidence being placed before judges and juries.

In the United States there has been a debate about the proper criteria for admitting evidence of novel techniques and theories.

In Britain proposals have been advanced for decreasing the role of juries where they are likely to be confronted with complex, conflicting, and esoteric evidence.

And in Australia, the Law Reform Commission has recently drafted new rules of evidence that will, if adopted, have a substantial impact on the range of scientific evidence coming before the courts. In July 2004, the federal Attorney-General asked the Commission to examine the operation of the Evidence Act of 1995. A series of Supreme Court decisions around Australia has edged toward adopting criteria for the reception of new forms of scientific evidence.¹⁴³

6.15.1.1.1 i. Investigating series of crimes

DNA profiling can be useful in providing the evidence of whether the same assailant is responsible for a series of crimes. This is particularly so in the case of serial rapes in which it is suspected that there is a single offender.

6.15.1.1.2 ii. Reopening unsolved cases

As DNA frequently maintains a useful degree of integrity in dried specimens for extended periods, the DNA profile can be used to re-evaluate old evidence that has not as yet, with the use of other techniques, been able to yield determinative or even useful evidence.¹⁴⁴

6.15.1.1.3 iii. Missing person and victim identification

In case of missing persons and victim identification¹⁴⁵, DNA profiling allows scientists to compare DNA patterns of unidentified people with those of their parents and to determine their identity definitely.¹⁴⁶

¹⁴³ Australian Law Reform Commission, <http://www.alrc.gov.au/> The Commission will release an Issues Paper in late 2004. A further consultation paper, containing draft proposals for reform, will be published in mid-2005. The final report is due to be delivered to the federal Attorney-General by 5 December 2005

¹⁴⁴ The Zaanse fitting room case of 1984 in The Netherlands illustrates the usefulness of DNA profiling, even years after the facts. It concerned the murder of a young shop assistant, who was found in one of the fitting rooms by a client. In 2002, 18 years after the murder, the police matched the blood on a knife they found in January 2002, to the blood of the murdered girl. Unfortunately, the owner of the knife, a drug addict, was already deceased, but his description corresponded to the picture witnesses painted in 1984.

¹⁴⁵ In the case Akkerman (The Netherlands) DNA profiling was successfully used to identify a murdered woman, 17 years after the facts. In 1983, the lifeless body of a woman was found. She was headless and the tops of all her fingers were cut off. They assumed it was the body of Ingrid Akkerman, who had disappeared few days before. She was about to file for divorce and therefore the husband was the prime suspect. However, there wasn't

Future of Identity in the Information Society (No. 507512)

6.15.1.1.4 iv. Paternity determination

Being able to establish the fatherhood can be of great importance from the perspective of payment of social security benefits and issues of inheritance. DNA technology is capable of resolving the uncertainty about a child's paternity even before it's born. This can be of major significance to sexual assault victims or women with multiple sexual partners. In Australia, DNA profiling has been included as a parentage test that can be ordered by the Australian Family Court.

In Belgian jurisprudence, a rare example of DNA evidence in court was delivered in 2001 in a case of paternity determination post mortem.¹⁴⁷

6.15.1.1.5 v. Immigration decision-making

In Britain, DNA profiling is regularly employed to screen immigrants requesting rights of residence on the basis of their familial relationship to current British citizens

The first reported use of DNA identification was in a non-criminal setting to prove a familial relationship. A Ghanaian boy was refused entry into the United Kingdom for lack of proof that he was the son of a woman who had the right of settlement in the U.K. Immigration authorities contended that the boy could be the nephew of the woman, not her son. DNA testing showed a high probability of a mother-son relationship. The U.K. Government accepted the test findings and admitted the boy.¹⁴⁸

6.15.1.2 Impediments of DNA as evidence

6.15.1.2.1 i. Tissue sampling powers

In many jurisdictions a significant impediment to the employment of DNA technology is the lack of police powers to compel suspects to provide a body tissue sample (usually blood) for analysis. Nevertheless, in the United Kingdom e.g. the securing of forensic evidence in breach with the law will not automatically render that evidence inadmissible. The courts have the duty to consider whether the balance of public interests requires them to exercise discretion to exclude evidence illegally obtained. There are two distinct elements to this discretion. The evidence may be excluded on the basis that its admission would have an unfair effect on the accused (primarily because it is unreliable) or alternatively, regardless of its effect at the trial, because of the manner of its extraction constituted unfair treatment of the accused. (the 'public policy' discretion).¹⁴⁹

The police have two distinct functions in the legal process. The first is an 'investigative function', encompassing the detection of the crime, the conducting of interviews and the

enough proof to convict him of the murder. In 2000, the daughter of Ingrid Akkerman requested a DNA examination. The investigation confirmed the presumptions of 1983.

¹⁴⁶ I. FRECKELTON, "DNA profiling – a legal perspective" in J. ROBERTSON (ed.), *DNA in forensic science: theory, techniques and applications*, New York, Ellis Horwood series in forensic science, 1990, 160.

¹⁴⁷ Luik, 27 November 2001, *J.L.M.B.* 2002, afl. 4, 156. Rb. Brussel, 28 juni 1988, *Pas.* 1989, III, 21.

¹⁴⁸ See K. KELLY, J. RANKIN and R. WINK, "Methods and Applications of DNA Fingerprinting: A Guide for the Non-Scientist," *Criminal Law Review*, 1987, 105 – 108.

¹⁴⁹ *Bunning v. Cross* High Court of Australia, 1978. This is a balancing task similar to that described in the Scottish case of *Lawrie v. Muir* of 1950: "The law must strive to reconcile two highly important interests (...) a) the interest of the citizen to be protected from illegal or irregular invasions of his liberties by the authorities, and (b) the interest of the State to secure that evidence bearing on the commission of crime and necessary to enable justice to be done shall not be withheld from courts of law on any merely formal or technical ground."

Future of Identity in the Information Society (No. 507512)

collection of evidence. The second is a ‘prosecutorial function’, encompassing the pursuit and detention of persons reasonably suspected of having committed offences and the bringing of such persons before the courts. The police are invested with distinct powers in each of these categories. The powers associated with one function are not to be used in the exertion of the other, e.g. in common law it is not allowed for the police to detain a suspect (a prosecutorial power) for the purpose of questioning (an investigative function). The collection of genetic material is part of the police force’s investigative function and therefore is subject to the limits placed by law upon that function.¹⁵⁰

In the United Kingdom, the power to take bodily samples in order to support a criminal prosecution originated in road traffic legislation. The Road Traffic Act 1988 contains the current powers of police to obtain such samples. The Act requires any person who is reasonably suspected of having committed driving offences premised upon the consumption of alcohol or drugs to provide a sample of breath, blood or urine.¹⁵¹

Prior to the Police and Criminal Evidence Act 1984 (PACE), a requirement to provide a specimen of breath for analysis was viewed as conflicting with the privilege against self-incrimination and as amounting to compelling evidence of a quasi-confessional nature. PACE, as amended by the Criminal Justice and Public Order Act 1994, now provides that non-intimate bodily samples and fingerprints are obtainable by compulsion and may be used for the purpose of a speculative search into criminal offending.¹⁵²

6.15.1.2.2 ii. Expert impact

If properly presented by its developers, DNA profiling is likely to be enthusiastically accepted by a criminal justice system hungry for the benefits that technology can bring to proof. But, without expert assistance, it is difficult to elicit the necessary information; the impact of the results of DNA profiling depend on the conclusions that experts are able to draw from them and most of the time, DNA results mean little without expert explanation to judge and jury.

The law places certain qualifications on the admissibility of such opinion evidence. The inferences that the expert draws from the factual results produced by scientific testing are themselves matters of opinion, not fact, and opinion is not admissible without further qualification. Evidence in court is normally restricted to the presentation of primary facts; the drawing of inferences is usually left to the judge or jury. An obvious exception to this rule occurs in the area of technical and scientific evidence with regard to which the judge or jury lack the necessary familiarity and expertise to interpret the material involved without expert assistance. In such cases, the opinion of properly qualified experts may be admissible to guide the judge or jury in drawing conclusions of their own.

The importance of the interpretation and appreciation of the evidence is underlined in the recommendations accompanying the second report of the American National Research Council in 1996, ‘The evaluation of forensic DNA evidence’:

“Recommendation 6.1.: behavioural research should be carried out to identify any conditions that might cause a trier of fact to misinterpret evidence on DNA profiling and to assess how

¹⁵⁰ S. EASTEAL, N. McLEOD and K. REED, *DNA profiling, principles, pitfalls and potential*, Chur, Harwood academic publishers, 1991, 27 – 28.

¹⁵¹ Road Traffic Act 1988 sections 3A, 4, 5, 6 and 7. It is an offence to fail, without reasonable excuse, to provide a specimen, RTA subsections 6(4) and 7(6).

¹⁵² Police and Criminal Evidence Act 1984 sections 61, 63, 63A, as amended by the Criminal Justice and Public Order Act 1994 sections 54 – 59.

Future of Identity in the Information Society (No. 507512)

well various ways of presenting expert testimony on DNA can reduce such misunderstandings.”

6.15.1.2.3 iii. Other aspects

Standard blood typing has been used for forensic purposes for many years. Where the conditions are optimal, DNA profiling will provide information of vastly increased utility. Standard blood typing can only be used with confidence in excluding some innocent suspects rather than in positively identifying a particular suspect as the offender. However, standard blood typing will continue to be used as an expedient preliminary screening device to exclude individual suspects and to narrow down a large field of possible suspects, because it is less costly and more rapid than DNA profiling.

However, as the use of DNA technology becomes more widely publicised, juries will come to expect it, like fingerprint evidence. This may put more pressure on prosecutors to use the technology whenever possible. Prosecutors must be trained on when to use the technology and how to interpret the results for the jury.¹⁵³

There is also the concern over the problems faced if the defence wishes to repeat tests carried out by the prosecution. Such problems may occur where the tests carried out by the prosecution have utilised all the available sample – and in the case of a crime scene sample this will be irreplaceable – or where the exact materials e.g. DNA probes used by the prosecution are not available to the defence for commercial or copyright reasons.¹⁵⁴

6.15.2 Fingerprints

Because friction ridge patterns on fingers are immediately obvious to simple visual examination, they were the first physical aspect of the personal identity to be perceived.

Fingerprint comparison does not require any biological material. The impression made by the papillary ridges on the ends of the fingers and thumbs is sufficient. To ensure privacy, provisions have been drawn up in the Netherlands governing storage of fingerprint identification data. Furthermore, fingerprint impressions are not made of every suspect apprehended but only for those who are in custody.

One impediment to data exchange and harmonisation of fingerprinting techniques is the criterion for identification. The problem is that though fingerprints do seem to be unique identifiers, any print must be read and matched. The question – one that can only be answered by rigorous scientific inquiry – is how much of a match is required to say that a particular fingerprint is from a particular person. For this purpose the so-called ‘dactyloscopic points’ are counted. The question at hand is how many points are considered necessary to identify the offender directly? Fingerprint experts had conceded that the process they use – matching large, evenly pressured prints taken from suspects at the police station to smaller, unevenly pressured prints from crime scenes – is ultimately subjective and bedevilled by inconsistent standards. The number of points needed for positive identification is not the same in all countries. There are even striking differences in the number required by the police and by the forensic laboratory within the same country. The French, for example, require that two fingerprints match at 16 points before they can be accepted as coming from the same person;

¹⁵³ E. CONNORS, T. LUNDREGAN, N. MILLER and T. McEWEN, US Department of Justice, *Convicted by juries, exonerated by science: Case studies in the use of DNA evidence to establish innocence after trial*, Alexandria, National Institute of Justice, 1996, 27.

¹⁵⁴ The Royal Commission on Criminal Justice, *The ability to challenge DNA evidence research study No 9*, London, HMSO, 1994.

Future of Identity in the Information Society (No. 507512)

the Australians, 12; and the Swedes, 7. In Australia, Canada and in the United States of America¹⁵⁵ there is no fixed number. This disparity in provisions can hinder exchange of data.¹⁵⁶

The 3rd U-S Circuit Court of Appeals in Philadelphia ruled in April 2004 the overall error rate in fingerprint examination to be microscopic, and claimed that most factors support admitting fingerprint identification evidence.¹⁵⁷ However, previous rulings show that jurisdiction has not yet come to agree upon the acceptance of fingerprints in court.¹⁵⁸

6.15.3 Handwriting identification

Handwriting is usually exercised with the fingers and hand, connected to the writer's body by his arm. Like the fingers and hand, the wrist and arm contain many nerves and muscles that can affect the writer before, during and after the act of writing.

Individuality is an extremely important concept and part of the handwriting identification process. By properly evaluating the significance of each feature, based on its rarity – or frequency of occurrence in random writings – and establishing the collective importance of those features when combined with the class characteristics of the writing, the expert is satisfied that the significance of the combination is unique enough to separate that writer from all others.¹⁵⁹

Individuality is often thought of as being more pronounced in a signature than in an extended writing. All the same, both can have a great deal of individuality, and frequently an extended writing is more identifiable than a signature because there is more opportunity for the writer to demonstrate his individuality.¹⁶⁰

¹⁵⁵ The F.B.I. refuses to state a number at all, relying instead on case- by-case judgments.

¹⁵⁶ L. VAN DER WESTEN, "Legal regulations governing forensic scientific methods" in J. F. NIJBOER and W. SPRANGERS (eds.), *Harmonisation in forensic expertise, an inquiry into the desirability of and opportunities for international standards*, Series criminal sciences, Amsterdam, Thela Thesis, 2000, 288 – 289.

¹⁵⁷ The case involved a 1991 heist in which a group of men was accused of taking \$20,000 from an armoured car driver in North Philadelphia. During the investigation, authorities allegedly discovered the prints of Byron Mitchell, the man accused of being the getaway driver, on a gearshift and driver's side door.

During a five-day hearing, Mitchell's attorneys presented testimony from expert witnesses who criticized techniques for using the partial fingerprint smudges left at crime scenes to identify suspects.

¹⁵⁸ *United States v. Havvard*, 2000; *United States v. Llera-Plaza*, 2002; *Regina v. Buckley*, Court of Appeal UK, 1999; *People v. James Hyatt USA*, 2000.

¹⁵⁹ From the point of view of forensic handwriting comparison, the key to the verification of the authenticity of questionable signatures lies in the reconstruction of the writing motion and its elements. The difference between genuine and copied signatures is based on the amount of pressure applied and on the structure of the writing line. Furthermore, the determination must reflect the observation that signatures from the same person may show different writing speeds.

¹⁶⁰ R. MORRIS, *Forensic Handwriting Identification*, London, Academic Press, 2000. Through the years, the following major principles of handwriting and hand printing identification have been established:

- 1 No two people write exactly alike.
 - 1.1.1 No one person writes exactly the same way twice.
 - 1.1.2 The significance of any feature, as evidence of identity or no-identity, and the problem of comparison, becomes one of considering a features rarity, the relative speed and naturalness with which it is written, and its agreement or disagreement with the feature(s) to which it can be compared.
 - 1.1.3 A writer is not able to imitate all the features of another person's handwriting or hand printing while simultaneously writing at the same relative speed and skill level as the writer he is seeking to imitate.

Future of Identity in the Information Society (No. 507512)

There are a number of court cases establishing the fact that the taking and providing of a handwriting sample for comparison purposes is not a violation of an individual's right against self-incrimination.¹⁶¹

In the *United States v. Jones*¹⁶² case in 1997, it was argued that handwriting identification ought not to be admitted because it could not be shown to be reliable. The United States Court of Appeal for the Eleventh Circuit rejected this thesis on 13 May 1999 in the *United States v. Paul*¹⁶³. In this ruling, the court held that the district court had properly admitted handwriting identification evidence as satisfying the 'scientifically reliable' criteria of the Daubert case.

Recently, two cases were decided by judges who, after carefully considering all of the prior judicial holdings, pro and con, came to the conclusion that the offered expert testimony on handwriting identification, including the ultimate opinion of a 'match', was fully admissible as meeting both the Daubert and the Kumho Tire requirements. The cases are *United States v. Prime*¹⁶⁴ (2002) and *United States v. Thornton*¹⁶⁵ (2003).

The Court of Appeal for the Fourth Circuit recently confirmed these judgments on 31 March 2003. The court handed down the decision of *United States v. Crisp*¹⁶⁶, holding that the expert testimony on handwriting comparison was admissible under the Daubert rules set by the United States Supreme Court.

Trial court rulings can reach one of the following three conclusions: (1) exclusion of all forms of expert testimony on handwriting comparison; (2) inclusion of the testimony on similarities and differences but exclusion of the expert's conclusions; and (3) inclusion of comparison and expert testimony.

In the majority of cases where handwriting evidence was challenged, the evidence was admitted as comporting with the Daubert/Kumho Tire criteria. In a few cases, the ultimate opinions of the experts were deemed not admissible although they were permitted to testify to

This is especially true the greater the relative speed the model writer uses. In simulating another's writing, the simulator will try to imitate those features that are most striking to his eye. He frequently either disregards those features that are less conspicuous to him or, if noted, fails to imitate them successfully.

1.1.4 For those writings where the writer successfully disguises his normal handwriting habits or where he imitates – traces – the writing habits of another writer while leaving no trace of his own, it is virtually impossible to identify the imitator.

¹⁶¹ Probably the most referred-to case is the case of *Gilbert v. California*, decided by the Supreme Court on 12 June 1967. The court held that, even though the defendant's attorney objected to the admission of requested handwriting specimens provided by his client on the grounds that they violated his Fifth Amendment right against self-incrimination and Sixth Amendment right to counsel, the court upheld the lower court's decision that the specimens provided had not violated his client's rights. The court cited *Schmerber v. California* where the court held that the Fifth Amendment offers no protection against compulsion to submit to fingerprinting, photographing, or measurements, to write or to speak for identification, to appear in court, to stand, to assume a stance, or to make a particular gesture.

In the case *Samual B. Lewis v. United States* (1967), the Supreme Court ruled the same way stating that written words used as a handwriting sample and not for its content doesn't automatically mean that the defendant had knowledge of a particular crime. The sample was only relevant for the shape of the letters and for the direction of some lines and marks, which may identify the writer in the same way as a fingerprint or photograph.

¹⁶² *United States v. Jones*, 107 F.3d 1147, 1160 (6th Cir. 1997)

¹⁶³ *United States v. Paul*, 175 F.3d 90.6 (11th Cir. 1999).

¹⁶⁴ *United States v. Prime*, 220 F.Supp.2d 1203 (W.D. Wash., Sept. 20, 2002).

¹⁶⁵ *United States v. Thornton*, F. Supp.2d, Case No. 02-M-9150-01, decided by the United States District Court for the District of Kansas on Jan. 24, 2003.

¹⁶⁶ *United States v. Crisp*, 324 F.3d 261 (4th Cir. 2003).

the similarities and differences between writing samples that had been studied. In only a few federal trial court decisions the judge ruled that the evidence of a forensic document examiner had to be fully excluded.

6.15.4 Voice identification (Speaker identification SPID)

The distinctiveness of people's voices is due to both physiological and behavioural differences in speech production. The physiological differences are due to the differences in the shape of the vocal tract. Behavioural differences are due to speaking style, and include aspects such as accents and language. The behavioural element means that even identical twins will have some differences in their voices.

There is a difference between voice identification and voice verification. The first one compares the voice of a test person with the voices of a certain group in order to identify the said person. The latter compares the voice of the test person exclusively with the available voice recording. From this perspective, forensic methods are an example of voice verification: it deals with the question whether the recorded voice is that of the suspect.¹⁶⁷

For example, there is the case in which a cop blackmailed financially wealthy persons at whom an investigation was directed. When he obtained appropriate evidence, he approached the suspect with promises to suppress the investigation, in return for hefty payments. Many of the 'victims' cooperated. However, some of them rebelled and, as a result, a series of tape-recorded telephone conversations were gathered. Subsequently, one needed to match the voice on these tapes with the cop's voice.¹⁶⁸

For the admissibility of voice recognition as evidence, the general rules of 'expert' testimony apply (Frye/Daubert). However, forensic voice identification cannot show an excellent record when it comes to value in the courtroom. A possible explanation can be found in the complexity of the speech signal for it displays an enormous amount of variations, which complicates the recognition by witnesses as well as the identification by experts. This variation is closely related to technical factors like variable recording conditions but also to the fact that speech – in comparison with biological characteristics like fingerprints or biological cellular material or even handwriting – contains an important behavioural component.¹⁶⁹

Therefore, a large amount of reticence is needed when introducing voice recognition by witnesses in court.

6.15.5 Ear print identification¹⁷⁰

The first famous ear print case took place in the United Kingdom in 1998. M. Dallager was convicted of murder on the basis of his ear print experts claimed he had left on the window of

¹⁶⁷ A. BROEDERS, *Op zoek naar de bron, over de grondslagen van de criminalistiek en de waardering van het forensisch bewijs*, Deventer, Kluwer, 2003, 379.

¹⁶⁸ H. HOLLIEN, *Forensic Voice Identification*, San Diego, Academic Press, 2002, 66 – 67.

¹⁶⁹ A. BROEDERS, *Op zoek naar de bron, over de grondslagen van de criminalistiek en de waardering van het forensisch bewijs*, Deventer, Kluwer, 2003, 403.

¹⁷⁰ The National Training Centre for Scientific Support to Crime Investigation (Harpeley Hall, County Durham) is in the process of compiling what is believed the world's largest computer database of ear prints to be used in the same way as fingerprint evidence in linking suspects to crimes. The aim is to build a comprehensive research tool to back up evidence that no two ears are exactly the same. The database has been built up using volunteers from among trainees at the centre and includes samples from identical twins, which are still different enough to be identifiable.

Future of Identity in the Information Society (No. 507512)

the victim's house, an elderly woman he had presumably murdered in 1996. He was sent to prison for life but cleared after 7 years because at retrial the prosecution failed to satisfy the court on the reliability of ear print evidence. Unlike the common practice in American courts, in the UK legal system, new or additional evidence can be represented for the first time on appeal. The former evidence had since been discredited and new DNA evidence had implicated a different person.

In 1999, the court of Appeal of Washington¹⁷¹ held ear print identification not generally accepted in the scientific community. It concerned an ear print on the bedroom door of the victim. The reasoning that the ear print is just another form of impression evidence and that other impression evidence is generally excepted in the scientific community as a means of making a positive identification – a statement testified by a Dutch police evidence technician¹⁷² – was overruled since a dozen acknowledged members of the forensic science community stated or implied the exact opposite. To come to this conclusion, the court stuck to the Frye-rule. As already mentioned, this rule provides that novel scientific, technical or other specialised knowledge may be admitted or relied upon only if generally accepted as reliable by the relevant scientific, technical or specialised community. General acceptance may be found from testimony that asserts it, from articles and publications, from widespread use in the community, or from the holdings of other courts. General acceptance is not at hand if there is a significant dispute between qualified experts as to the validity of scientific evidence, as was the case in this court case. After years of imprisonment, the suspect's conviction was reversed.

Although the generalised principle of uniqueness which states that 'nature never repeats itself' is probably true, the principle cannot substitute a systematic and thorough investigation of a physical evidence category. First, it needs to be statistically shown that no two ears are alike.¹⁷³ Ear prints of the same ear vary according to the angle and rotation of the head and also according to the degree of pressure with which the head is pressed against the receiving surface. So, even if each ear is different, it still must be established that the print of an ear is an accurate enough presentation of the actual ear to be useful as a means of identification.¹⁷⁴

The issue of ear evidence also surfaced in The Netherlands¹⁷⁵, in a different context however because it dealt with the comparison of the ear detail visible in a photograph taken by a surveillance camera with ear photographs taken of a suspect. Technically, it would seem that the identification of an individual by ear characteristics visible on a photograph would offer a better chance for a meaningful comparison since pressure distortion, prevalent in ear

¹⁷¹ *State v. David Wayne Kunze*, Court of Appeal of Washington, Division 2, 97 Wash. App. 832, 988 P. 2D 977 (1999).

¹⁷² Cornelius VAN DER LUGT, a law enforcement person and not a scientist who also testified in the Dallagher case in the UK, is supported in his vision by Alfred IANNARELLI who stated that "ear print identification is an exact science that can be used to prove beyond any reasonable doubt and to a mortal certainty that an unknown ear print found at the scene of a crime is that of the know suspect." However, these statements lack an adequate factual backing.

¹⁷³ As C. CHAMPOD, formerly a professor at the University of Lausanne, Switzerland, and a scientist employed by the British Forensic Science Service testified in the Kunze Dallagher case: "A high variability between ears does not imply necessarily that a high variability is expressed in marks left by different persons."

¹⁷⁴ T. EGAN, "Are Dutch ears different from American ears? A comparison of evidence standards.", http://forensic-evidence.com/site/ID/ID00004_1.html.

¹⁷⁵ Case No. 23-001847-99, verdict No. 948/00, Court of Appeal of Amsterdam, 8 May 2000: "The court has especially considered that the determinative proof in this case was based upon an ear identification, which, in the current state of the development in forensic science and forensic knowledge should be considered with caution and reservations. On that issue it is the court's opinion that the result of the ear identification inquiry finds insufficient support accepted evidentiary principles."

Future of Identity in the Information Society (No. 507512)

impressions left upon hard surfaces such as a door or a window, would not be present to complicate the side-by-side comparison. However, the decision of the court emphasised in its opinion that ear identification lacked acceptance in the forensic community.

Nevertheless, the point of departure of the latter case is interesting for in many countries, the use of surveillance cameras has grown explosively. As a consequence, an increasing number of crimes are recorded on video by surveillance cameras. Nowadays, the question of identifying persons on the tape is put to the forensic expert more and more frequently.¹⁷⁶

For the time being, ear print comparison can help to narrow the field; it may eliminate but cannot alone be regarded as a safe basis on which to identify a particular individual as being the person who left one or more prints at the crime scene.¹⁷⁷

6.15.6 Lip print identification

There are few mentions of lip print identification cases in literature, however in May 1999, an Illinois Court of Appeal accepted the testimony of two state police experts stating that lip print identification is generally acceptable within the forensic science community as a means of positive identification; stating that lip print identification methodology is very similar to fingerprint comparison and that it is a known and accepted form of scientific comparison.¹⁷⁸

A. MOENSSENS however concluded that lip prints are not a viable means by which an investigator may identify an individual.¹⁷⁹

6.15.7 Facial recognition

Facial recognition programs have been criticised for their inaccuracies and unreliability. The digitised photographs are highly susceptible to changes in lighting and facial positioning. Furthermore, the system may not pick up a match if the picture in the database is two or more years old since the technology has a difficult time recognising the effects of aging. Different hairstyles, the addition of facial hair, or glasses may also fool the system¹⁸⁰.

6.15.8 Iris recognition and retina

First of all, we should note the existence of two separate methods of making use of the eye as a biometric. Iris Recognition, the newer approach, takes images of the visible, coloured, part of the eye and processes these into templates called iris-codes. With life detection algorithms based on pupil reactions, it is theoretically possible to determine someone's medical situation (for example if someone is influenced by drugs or alcohol).

An older and very different approach, which is no longer being actively marketed, is retinal scanning. Retinal scanning requires considerably more co-operation from the user, imaging

¹⁷⁶ A. HOOGSTRATE, H. VAN DEN HEUVEL and E. HUYBEN, "Ear identification based on surveillance camera's images", May 2000, <http://forensic-evidence.com/site/ID/IDearCamera.html>

¹⁷⁷ A. MOENSSENS and D. STRIPP, "Another ear print conviction reversed! UK Court of Appeal orders new trial – New trial halted!", June 2004, http://forensic-evidence.com/site/ID/dallangher_UK.html

¹⁷⁸ *People v. Davis*, Court of Appeal of Illinois, 12 May 1999, No. 2-97-0725.

¹⁷⁹ A. MOENSSENS, STARRS and HENDERSON, *Scientific evidence in civil and criminal cases*, Foundation Press, 1995, 611.

¹⁸⁰ <http://www.itl.nist.gov/iad/894.03/face/face.html>

Future of Identity in the Information Society (No. 507512)

the pattern of red blood vessels behind the eyeball and requiring more sophisticated optical instruments.¹⁸¹

6.15.9 Bite mark identification

In 1991 a bite mark on the victim along with blood from a very common blood type, was the only thing the police had to work with. According to a state forensic orthodontist, the marks matched the dentition of the suspect who was subsequently branded the ‘snaggletooth killer’ and sentenced to death. In 2002, by the time DNA testing was done routinely on behalf of the prosecution, the case was reopened before the Supreme Court of Arizona and examination of the saliva contained in the bite mark not only cleared the convict but also identified the true perpetrator – a person already incarcerated on another unrelated offence – through a search in the DNA database.¹⁸²

6.15.10 Conclusion

There are few legal regulations governing forensic examination. Many countries have framework legislation for certain scientific areas and set requirements for forensic expertise in that area.

Most methods of forensic expertise are unregulated by law. Frequently, forensic scientists work to the stringent standards fully accepted and laid down in their area of expertise; however these regulations do not have the force of law. Many forensic examinations, in particular identifications, involve data sensitive from the perspective of personal privacy and are therefore subject to privacy legislation. The court will certainly take regulations laid down by the profession into consideration in its assessment of a method of analysis.

6.16 Forensic Identification databases

The areas of forensic science are defined according to the type of trace they deal with. Databases have been developed for separate domains (biological evidence, fingerprints, marks, trace evidence, etc.), generally automating tasks that were previously carried out manually on large collections of data. Our focus is on forensic databases that provide the ability to associate recovered evidence with an individual (or a list of potential candidates) either directly or indirectly.¹⁸³

6.17 Privacy and the use of databases¹⁸⁴

The evolution of technology in the last decade makes it possible to store enormous amounts of data in databases. It is therefore theoretically possible to collect and keep different sorts of data about the entire population of a country. One can imagine developing a forensic identification database containing DNA information, blood samples, tissue or fingerprints of

¹⁸¹ BioVision, Roadmap for Biometrics in Europe to 2010, October 2003, <http://db.cwi.nl/rapporten/abstract.php?abstractnr=1411>.

¹⁸² *State v. Krone*, 182 Ariz. 319, 897 P.2d 621 (*en banc*, 1995).

¹⁸³ Some examples are databases for fingerprints, shoeprints, projectiles (land and groove impressions) and cartridge casings (breach face and firing pin impressions), handwriting and DNA profiles.

¹⁸⁴ D. ALONSO BLAS, “Privacy and use of data-bases in forensic disciplines” in J. F. NIJBOER and W. SPRANGERS (eds.), *Harmonisation in forensic expertise, an inquiry into the desirability of and opportunities for international standards*, Series criminal sciences, Amsterdam, Thela Thesis, 2000, 499 – 511.

Future of Identity in the Information Society (No. 507512)

every citizen to facilitate forensic research.¹⁸⁵ Some jurisdictions even have mandatory procedures to deposit the DNA of convicted criminals into their DNA database for matching against DNA material recovered from unsolved crimes. Supporters of these systems note that DNA identification is vital in the solution of some cases.¹⁸⁶

6.17.1 United States

In March 1999 US Attorney General Jaret Reno asked a federal commission to study the possibility of requiring a DNA sample to be collected from every person arrested in the US (even for minor violations) and to be permanently stored in a national database.¹⁸⁷ This national database would undoubtedly facilitate the investigation of crime and offences. However, American civil libertarians protested against the increased collection of DNA data, arguing that it constitutes an illegal search with little purpose in most cases, especially for minor crimes. They therefore challenged the proportionality of the whole project.

6.17.2 European Union

In Europe we have a long tradition of data protection or privacy protection. One of the first examples is the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of 1981.¹⁸⁸ This convention, which was the first and only legally binding international instrument of world-wide significance, draws inspiration directly from the European Convention of Human Rights and Fundamental Freedoms, which was opened for signature in 1950.¹⁸⁹

A resolution of the Council of the European Union dating from 9 June 1997 regulates the exchange of DNA analyses results. It touches the subject of DNA databases as well, stating

¹⁸⁵ In Iceland the government recently proposed creating a centralised electronic database containing health records and other related information, including genetic data, in principle relating to Icelanders, for the purpose of monitoring the use of medical services and pharmaceutical products. The intended purpose of this database was to increase knowledge in order to improve health and health services a legitimate aim, one might think at first glance. However, it is not so simple to draw this conclusion since other interests of those whose data are processed could be at stake. The envisaged database was supposed to contain anonymous data but in a country with a relatively small population, genetic information is likely to indicate biological lineage and to reveal identities of persons concerned. The security measures initially proposed by Iceland to replace identifiers by a code were not sufficient to guarantee the anonymity of the Icelandic population.

¹⁸⁶ An extremely large DNA identification databank has been constructed by the US Department of Defence (DoD). The purpose of the Department of Defence DNA Registry is to identify the remains of lost soldiers. As of 2001, the Registry's Specimen Repository had an estimated 3.5 million DNA specimens. Many other DNA storage systems exist, but are not presently being used for identification purposes. These include research databases, blood banks and tissue storage facilities. In spite of the fact that these systems are not primarily identification systems, care should be taken in the design, architecture and policy development of these systems since the potential exists for new technology to allow these DNA samples to be used to profile and identify individuals. Document of the OECD (Organisation for Economic Co-operation and Development) Working Party on Information Security and Privacy about Biometric-based technologies, 30 June 2004, www.oecd.org/sti/security-privacy.

¹⁸⁷ See EPIC alert 6.04, 4th of March 1999, <http://www.epic.org>. Such a database would be extremely large since almost 15 million people are arrested in the US yearly.

¹⁸⁸ Council of Europe, European Treaties Series, No. 8, *Explanatory Report on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Convention opened to signature on 28 January 1981, Strasbourg: 1981.

¹⁸⁹ See <http://www.coe.fr/dataprotection>.

Future of Identity in the Information Society (No. 507512)

that it is up to the Member States to decide on the conditions under which, and the offences regarding which, the DNA analysis results may be stored in a national database.¹⁹⁰

The European Data Protection Directive of 1995¹⁹¹ offers a set of principles and provisions for implementation in all countries of the Union. Most of these countries (with the exception of Italy and Greece) had already enacted privacy legislation before the adoption of the Directive but this legislation presented some substantial differences, which jeopardised to some extent the free flow of personal data within the European Union.

6.17.2.1 Personal data

Most of the data necessary for forensic research can be qualified as personal data. A definition of this concept is contained in article 2 (a) of the European Data Protection Directive: “All information relating to an identified or identifiable natural person”.

“All information relating to” covers all data, which can furnish information about a defined person. It is not necessary to know the name of a person to speak of personal data; it is enough if the data make it possible to identify this person. Someone is identifiable who can directly or indirectly be identified.¹⁹²

The data protection directive has distinguished a special category of data called sensitive data; article 8 prohibits in general the processing of data such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and the processing of data concerning health or sex life. The reason for this special protection is found in the preamble of the Directive referring to sensitive data as “data which are capable by their nature of infringing fundamental freedoms or privacy”.

Some of the data that are regularly used for forensic research belong to the category of sensitive data since they somehow concern the health of natural persons; for instance, blood or tissue samples or DNA data.

6.17.2.2 Legitimate grounds for processing personal and sensitive data

The European Privacy Directive defines processing in article 2 (b) as “any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alternation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction”.

To ensure that the processing of personal data occurs in a legitimate way, processing can only take place in one of the circumstances defined in article 7 of the European Directive. In the context of forensic research the following grounds could play a role:

¹⁹⁰ Council of the European Union, Resolution on the exchange of DNA analysis results, 9 June 1997, *Official Journal* C 193, 24 June 1997, p. 0002 – 0003.

¹⁹¹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *O.J. L.* 281, Volume 38, 23 November 1995. Entered into force on 25th of October 1998.

¹⁹² Common and well-known examples of data used in forensic research which can be clearly qualified as personal data are e.g. the sperm samples found on Monica Lewinsky’s famous blue cocktail dress which matched the DNA features of President Clinton and another one is the shoeprint found near the place where O.J. Simpson’s wife was killed. Examination proved that these shoeprints could only belong to very specific and exclusive sport shoes. O.J. Simpson had by chance been photographed some weeks before the death of his wife wearing shoes of this kind, although he later denied ever having owned these shoes...

Future of Identity in the Information Society (No. 507512)

- Unambiguous consent: if a suspect or a victim of a crime or offence collaborates with the investigators and agrees to the investigation, it is clear that his/her personal data can be legitimately collected and processed.
 - Consent means that the data subject must be absolutely free to consent and have enough information before taking a decision; only then one can speak of free and informed consent.
 - A person who is considered a suspect of a crime or offence is not totally free to decide whether or not to co-operate with the forensic researchers. Caution is therefore necessary when using the term consent in this context.
- Compliance with a legal obligation to which the controller is subject: for instance, in The Netherlands, in case of DNA data, there is the legal obligation to keep these data in the national data bank of genetic profiles when dealing with suspects of offences punishable by a penalty of imprisonment of eight years or more.¹⁹³
- Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Some of the data regularly used for forensic research belong to the category of sensitive data so that processing is only legally permitted when one of the following exceptional grounds plays a role:

- Explicit consent of the data subject: if a suspect or a victim of a crime or offence gives explicit consent to the researchers, personal data can be processed, even if they belong to the category of sensitive data. However, the limited freedom of a suspect when giving consent should be taken into consideration.
- Necessary for the establishment, exercise or defence of legal claims: even without the consent of the data subject – who in many cases remains unknown to the researchers at the moment of processing of the data – sensitive data can be processed in a crime investigation when they can serve to establish, exercise or defend a legal claim.

Article 8, paragraph 4 of the European Directive enables the Member States to lay down other exemptions for reasons of substantial public interest and subject to the provision of suitable safeguards. It is therefore necessary to assess whether the benefits of forensic research are important enough to constitute substantial public interest. This assessment is up to the national legislator.

The Council of Europe issued a Recommendation on 23 January 1981¹⁹⁴ in which it expressed its concern about the risk of increasing use of computers for, among others, medical research.

¹⁹³ Law of 8th of November 1993, which incorporated new provisions in the criminal code dealing with DNA research in criminal cases, *Official Journal* 1993, 596; Royal Decree of 4 July 1994 on DNA research, *Official Journal* 1994, 522; Regulation of the Minister of Justice on DNA research, *Official Journal*, 1994, 174.

¹⁹⁴ Council of Europe, Recommendation No R(81) 1 adopted by the Committee of Ministers of the Council of Europe on 23 January 1981, *Regulations for Automated Medical Data Banks*, Strasbourg, Legal Affairs Committee, 1981.

Future of Identity in the Information Society (No. 507512)

In 1997¹⁹⁵ a new Recommendation on the protection of medical data was adopted. In the context of this Recommendation, medical data are defined as all personal data concerning the health of an individual. It also refers to data that have a clear and close link with health as well as to genetic data. According to the Recommendation, medical data can only be collected and processed if in accordance with appropriate safeguards provided by domestic law. Therefore the circumstances, under which the collection and processing of medical data is allowed, are quite limited. In the context of forensic research, the following grounds can be invoked:

- If provided by law: for the prevention of a real danger or the suppression of a specific criminal offence or some other public interest.
- If permitted by law: to safeguard the vital interests of the data subject or a third person, or to establish, exercise or defend a legal claim.
- If the data subject (or his/her representative or a body or authority provided by law) has given consent.

The processing of genetic data is subject to specific safeguards: processing of these data for the purpose of a judicial or a criminal investigation should be subject to a specific law offering appropriate safeguards.

When in the legitimate interest of public health or medical science, the person in charge of the medical treatment or the controller of the file deems it necessary to – in order to enable him/her to defend or exercise a legal claim – store medical data that no longer serve their original purpose, technical arrangements should be made to ensure their correct storage and security, taking into account the privacy of the patient.

An authorised forensic laboratory usually carries out forensic investigations. The work of these laboratories falls obviously within the scope of the existing privacy legislation. However, once the data have been transferred from the forensic laboratory to police or justice agencies – those who can use these data for criminal investigation or proceedings – the situation changes.

The European Data Protection Directive defines its scope of applicability in article 3, excluding the processing of personal data concerning public security, defence, State security and the activities of the State related criminal law.¹⁹⁶

¹⁹⁵ Council of Europe, Recommendation No R(97) 5 of the Committee of Ministers to Member States on the protection of personal data, adopted by the Committee of Ministers on 13 February 1997 at the 548th meeting of the Ministers' Deputies.

¹⁹⁶ See also Recital 13 of the preamble of the Directive. The reason for this exclusion lies in the organisation of the European Communities or, more accurately, in the Treaty of Maastricht on the European Union. The Member States have transferred a large number of competencies to the EU, retaining certain activities which they consider inherent to their national identity or sovereignty, such as defence, police and penal matters (the so-called third pillar activities). For this reason the Data Protection Directive cannot regulate areas that fall outside the scope of application of European Law in general. However, this does not mean that no data protection rules apply to the third pillar activities. Member States are free to extend the protection of the Directive to the data processing activities in this field.

6.18 Dangers?

The potential for misuse is worrying, not in the least because DNA samples may reveal genetic conditions and perhaps even genetic markers for aggression, substance abuse, mental illness, criminal tendency and so on. This genetic information is relevant not only to the individual whose sample is being taken, but also to those who are related to that individual. The fear is that even strict controls on the dissemination of this information may not, ultimately, prevent the data being used for purposes unconnected with the investigation of a crime.¹⁹⁷

6.19 Conclusion

Since the September 11 attacks in the USA, the public outcry for better and more universally available identification technology has been significant and several countries have responded with legislation mandating not only better security but achieving that result using high-tech biometrics devices in airports and in immigration offices. While the risk of privacy infringement is still the most compelling argument against the widespread use of biometric technology in law enforcement, this view tragically seems to hold less weight today, in light of the recent tragedies. However by using the biometric properties in an insecure way, the risk exists that the forensic value of a given biometrics is less identifying, since this property is known and can be copied from other databases¹⁹⁸.

The need for digital forensics training and laboratories is beginning to be recognised and met. Much effort and specialised training of law enforcement and forensic experts over the years have developed the process of preserving and analysing forensic evidence – fingerprinting, hair and blood analysis, DNA, ballistics, ... – a process that criminal law has come to rely on today. Likewise, more training and resources are needed, especially in the form of more laboratories and research centres, for the practice of criminal law to benefit from electronic forensic evidence in the future.

All this potential will only be valuable if prosecutors ensure law enforcement investigators and technical analysts follow the necessary protocols. In doing so, prosecutors can ensure that otherwise admissible electronic evidence is not suppressed or compromised legally either because of an illegal search and seizure or because the evidentiary foundation was not properly or credibly laid during trial.

The focus of most of the current legislation and judicial activity determines the admissibility of the evidence in broad terms. However, a clearer and universal legislative approach of the admissibility of forensic evidence could be of great importance, all the more keeping in mind the huge progress in the field of forensic science and its growing importance in the judicial world.

¹⁹⁷ S. SHARPE, *Search and surveillance, the movement from evidence to information*, Hants, Dartmouth Publishing Company Limited, 2000, 205.

¹⁹⁸ 'FIDIS Deliverable 2.1', available at <http://www.fidis.net>

7 Conclusion

This work has been an overview of issues that arise from different perspectives of Identity Management Systems and their forensic implications. As has been shown, information from digital systems can be useful as evidence in the court, however it is important to be aware that identities can be stolen or 'borrowed' in the case of a mobile device, and devices such as biometric systems do not always function as expected for technical, management or other reasons.

Although the information that is extracted from such systems can be used as evidence in court, for forensic science, it is important to give a statement of the technologies' limitations and thus how strong or weak the evidence alone is. As such, it is important to also consider other available evidence. With many systems there exists a possibility of incorrect association of a user with a mobile device, deliberate tampering with the system or system error through incorrect usage or technical faults. A classic example is that fingerprints can be spoofed, and indeed other biometric features can be copied, even without the owner of that feature knowing it. Additionally, the claims from the manufacturers of the devices should always be verified. If they claim a device has liveness detection for example, this should be checked. For these reasons, in the examination process, it is important to consider the likely integrity of the data, i.e. how failsafe the system is, since this could provide an alternative hypothesis such as a different individual being involved in the crime. Equally, it is necessary to ensure law enforcement investigators and technical analysts follow the necessary protocols. In doing so, prosecutors can ensure that otherwise admissible electronic evidence is not suppressed or compromised legally either because of an illegal search and seizure or because the evidentiary foundation was not properly or credibly laid during trial.

The next step: More Identity Management Systems should be covered in depth concerning their merits for forensic information extraction.

Since Identity Management Systems often have databases behind them, these databases can be combined, and by using profiling techniques more information concerning a crime can be found in the databases. In FIDIS Deliverable 6.2 ('Thematic workshop on forensic implications' in September 2005) we have begun to focus on associated profiling issues, and as such, the next deliverable within this workpackage will also focus on these aspects.

8 Glossary

Back Door

A hardware or software hidden entrance to a computer system’s security policies.

False Acceptance Rate/FAR

The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. The rate given normally assumes passive impostor attempts. The False Accept Rate may be estimated as

$$FAR = NFA / NIIA$$

or

$$FAR = NFA / NIVA$$

where

FAR	is the false acceptance rate
NFA	is the number of false acceptances
NIIA	is the number of impostor identification attempts
NIVA	is the number of impostor verification attempts

False Rejection Rate/FRR

The probability that a biometric system will fail to identify an enrollee, or verify the legitimate claimed identity of an enrollee. The False Rejection Rate may be estimated as follows:

$$FRR = NFR / NEIA$$

or

$$FRR = NFR / NEVA$$

where

FRR	is the false rejection rate
NFR	is the number of false rejections
NEIA	is the number of enrollee identification attempts
NEVA	is the number of enrollee verification attempts

This estimate assumes that the enrollee identification/verification attempts are representative of those for the whole population of end-users. The False Rejection Rate normally excludes ‘Failure to Acquire’ errors

Equal Error Rate

The error rate occurring when the decision threshold of a system is set so that the proportion of false rejections will be approximately equal to the proportion of false acceptances

IMEI

International Mobile Equipment Identity

Future of Identity in the Information Society (No. 507512)

IMSI

International Mobile Subscriber Identity; an internal subscriber identity used only by the network

PGP

Software for encryption; Pretty Good Privacy www.pgp.com

SIM

Subscriber Identity Module; A smart card containing the telephone number of the subscriber, encoded network identification details, the PIN and other user data such as the phone book. A user's SIM card can be moved from phone to phone as it contains all the key information required to activate the phone

Trojan

A trojan horse is called to refer to the story of the Greek legend. It is a malicious program disguised as a normal application

Virus

A malicious code that replicates itself

Worm

A worm is similar to a virus. They replicate themselves like viruses, but do not alter files, like viruses do. The main difference is that the worm resides in memory.