Biometrie in Zeiten von eIDs, Social Networks und Cloud Computing – die Datenschutzsicht

Marit Hansen*)
Unabhängiges Landeszentrum für Datenschutz
Schleswig-Holstein

Berlin, 30.11.2012
Workshop „Biometrische Identitäten und ihre Rolle in den Diskursen um Sicherheit und Grenzen“

*) Ein besonderer Dank gilt Dr. Martin Meints und Dr. Thomas Probst (ULD) für einige Folien.

Roter Faden

- Datenschutz
- Biometrie
- Biometrie & Datenschutz
  - Biometrie in eIDs – die Datenschutzsicht
  - Biometrie in Sozialen Netzwerken – die Datenschutzsicht
  - Biometrie in der Cloud – die Datenschutzsicht
  - Weitere Entwicklungen
- Fazit

Datenschutz

Recht auf informationelle Selbstbestimmung

- Datenschutz-Grundrecht:
  „Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen“
- Jeder soll wissen können, wer was wann über ihn weiß.
- Anlass: Volkszählung
- Bundesverfassungsgericht: Urteil vom 15. Dezember 1983 (BVerfGE 65, 1)
- Ähnlich: Alan F. Westin, 1967

Zu wenig Datenschutz
⇒ Eingriff in Persönlichkeit

- Motivation der Verfassungsrichter beim Volkszählungsurteil 1983
- Ähnliche Argumentation 2008 beim Urteil zur Online-Durchsuchung

Die 7 Regeln des Datenschutzes

1. Rechtmäßigkeit
2. Einwilligung
3. Zweckbindung
4. Erforderlichkeit und Datensparsamkeit
5. Transparenz und Betroffenenrechte
6. Datensicherheit
7. Kontrolle

Die 7 Regeln des Datenschutzes

1. Rechtmäßigkeit
2. Einwilligung
3. Zweckbindung
4. Erforderlichkeit und Datensp
5. Transparenz und Bet enrechte
6. Datensicherheit
7. Kontrolle

Für jede Datenverarbeitung ist eine rechtliche Grundlage nötig, z.B. Gesetz, Vertrag, Einwilligung.

Einwilligung bedeutet: Der Betroffene wurde ausreichend informiert und hat freiwillig eingewilligt.

Personenbezogene Daten dürfen nur für den angegebenen Zweck verwendet werden.

Die 7 Regeln des Datenschutzes

1. Rechtmäßigkeit
2. Einwilligung
3. Zweckbindung
4. Erforderlichkeit und Datensparsamkeit
5. Transparenz und Betroffenenrechte
6. Datensic
7. Kontroll

Es dürfen nur die personenbezogenen Daten verwendet werden, die für den jeweiligen Zweck erforderlich sind.

Die Daten müssen gelöscht werden, sobald sie nicht mehr benötigt werden.

Erhebung und Verarbeitung personenbezogener Daten muss gegenüber Betroffenen transparent sein.

Betroffene haben Rechte auf Auskunft und Berichtigung sowie (eingeschränkt) auf Sperrung und Löschung.

Die 7 Regeln des Datenschutzes

1. Rechtmäßigkeit
2. Einwilligung
3. Zweckbindung
4. Erforderlichkeit und Date[illegible]samkeit
5. Transparenz und Be[illegible]offenenrechte
6. Datensicherheit
7. Kontrolle

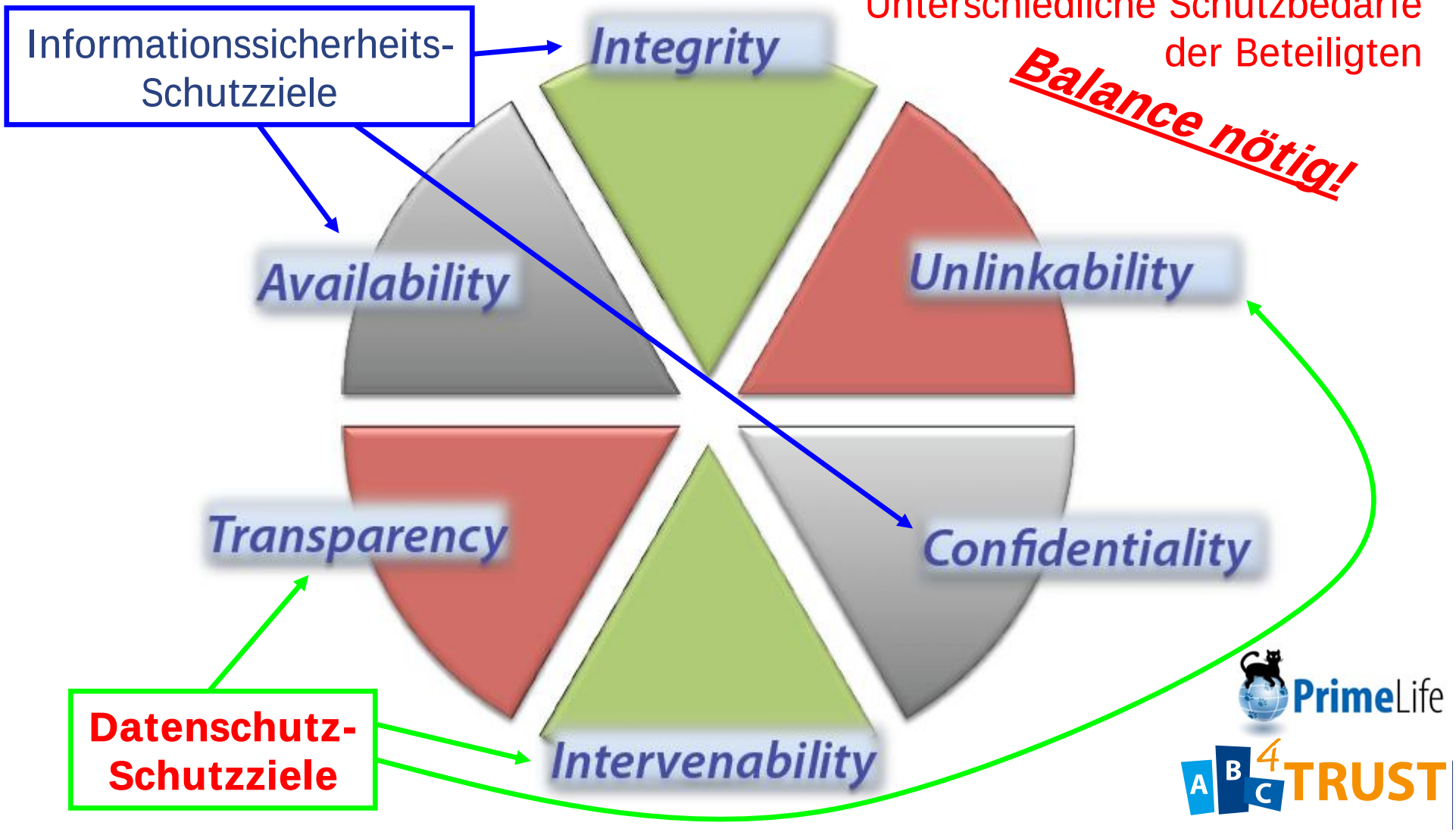
Unberechtigte Zugriffe auf die Daten müssen durch technische und organisatorische Maßnahmen ausgeschlossen werden.

Die Datenverarbeitung muss einer internen und externen Kontrolle unterliegen.

Kombination von Schutzzielen der Informationssicherheit und des Datenschutzes

Unterschiedliche Schutzbedarfe der Beteiligten

Balance nötig!

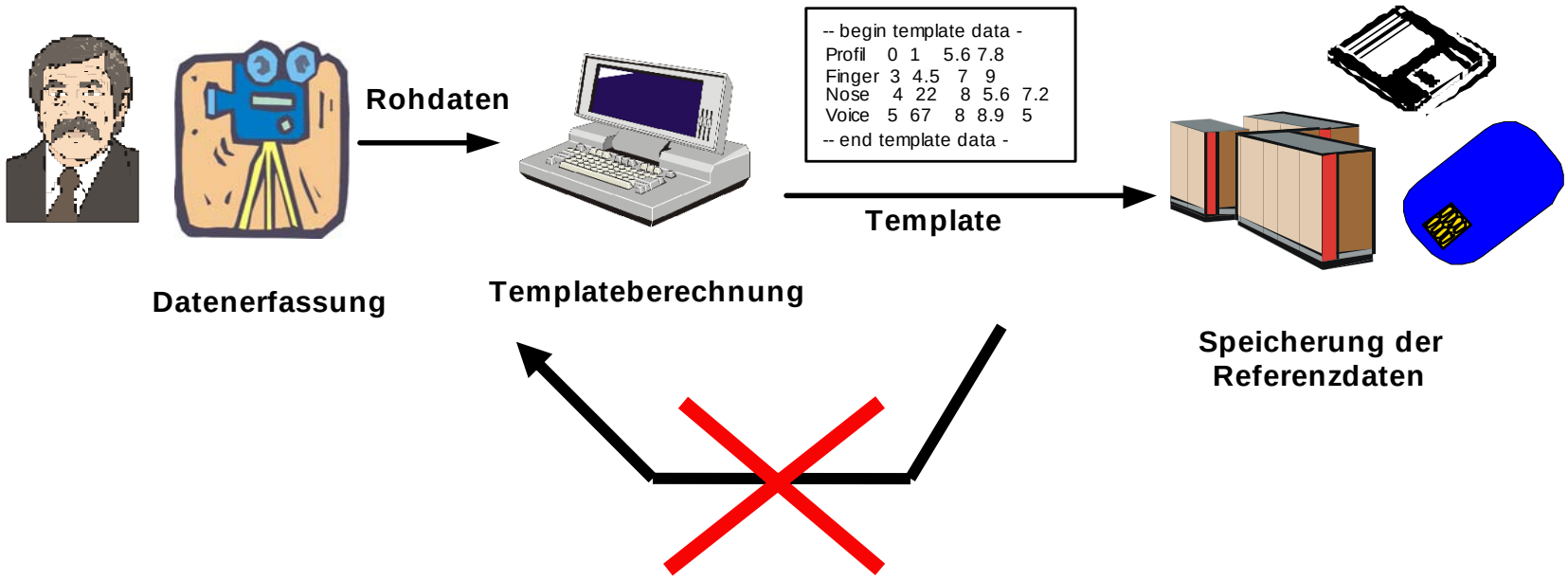


PrimeLife

ABC4TRUST

Biometrie

Funktionsweise

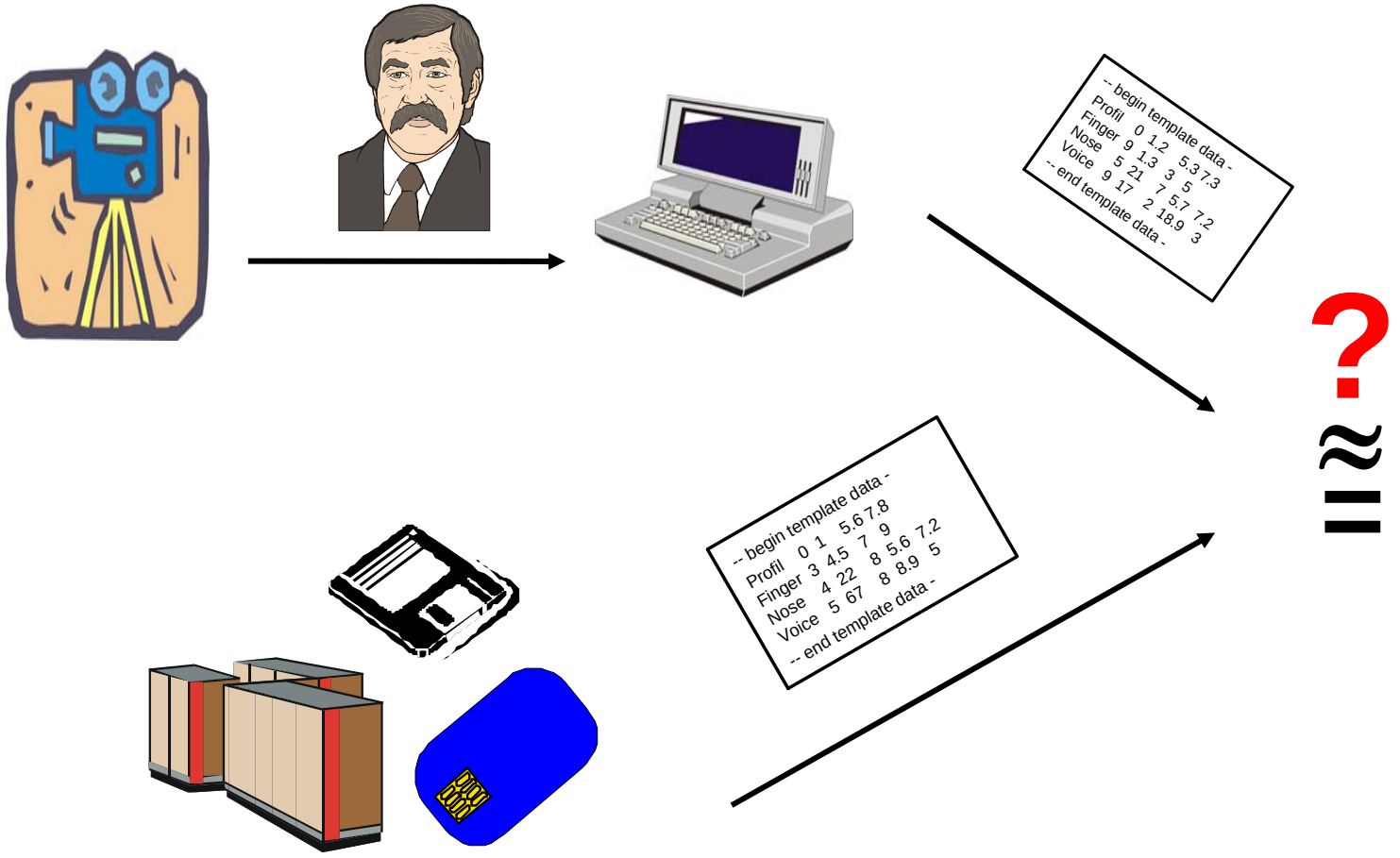


Beispiel: Finger-abdruckerkennung

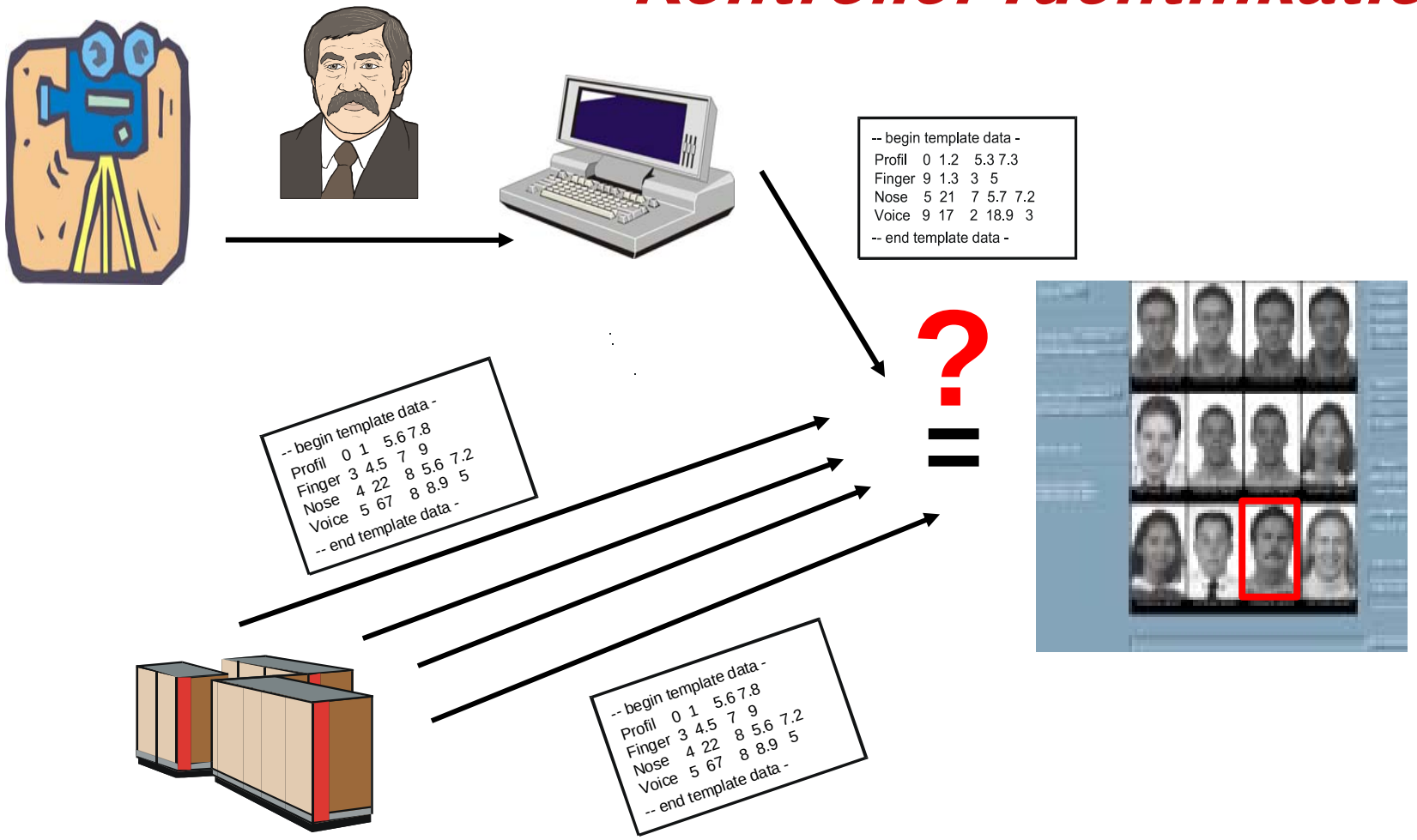
Minutien

Kuhn, Markus: Security – Biometric Identification.
http://www.cl.cam.ac.uk/Teaching/2003/Security/guestslides/slides-biometric-4up.pdf

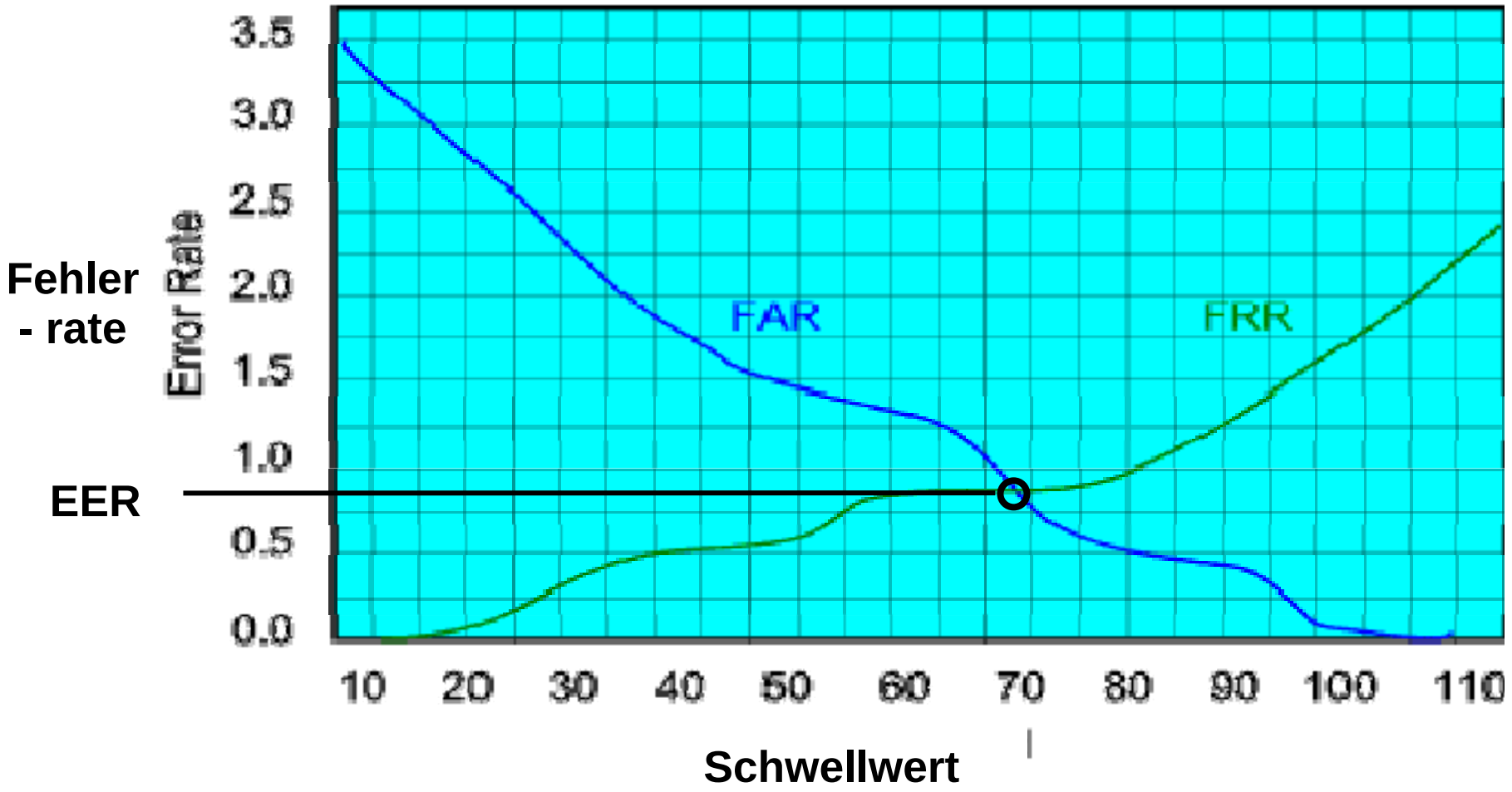
Kontrolle: Verifikation



Kontrolle: Identifikation

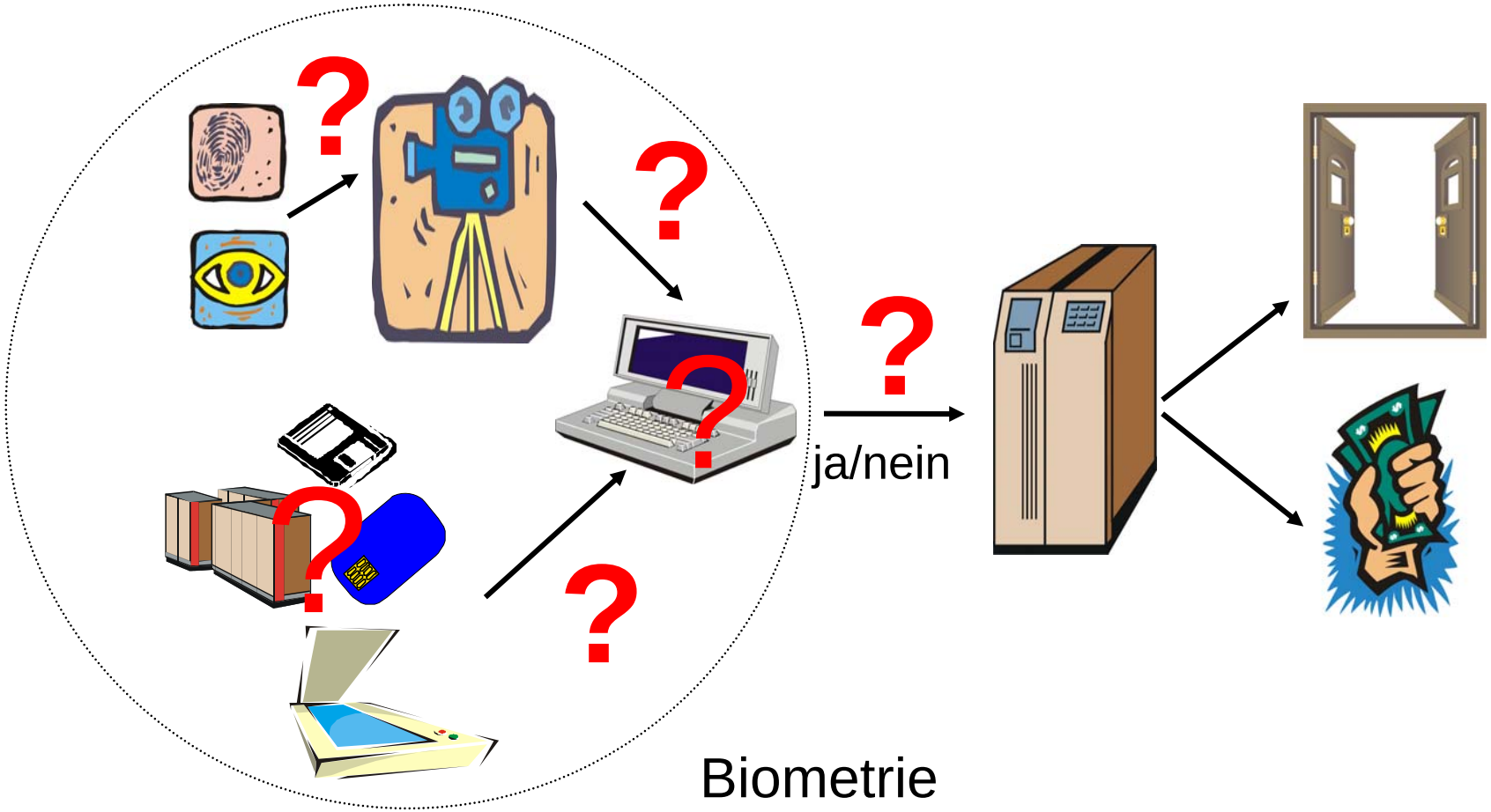


Fehlerraten



Biometrie & Datenschutz

Sicherheit: Angriffspunkte



Biometrie

Die Datenschutzsicht I

- Lebenslange Bindung der Daten
  - Keine effektive „Rückrufmöglichkeit“
  - Solange keine Beimischung von Zufallsdaten: Verkettungsrisiko
- „Überschießende Informationen“ in Rohdaten
  - Weitere Analysemöglichkeiten, z.B. zu Krankheiten, Verhalten, Stimmung, ethnischen Hintergründen etc.
  - Ausschluss überschießender Informationen ist wenig erforscht
- Vielfach: heimliche Überwachung ermöglichend
  - Wenn wissentliche Mitwirkung des Betroffenen nicht nötig
- Vielfach: Zweckbindung der Daten nicht effektiv zu gewährleisten

⇒ **Nicht-Verkettbarkeit?**

Die Datenschutzsicht II

- „Automatisierte Einzelentscheidungen“
  - Biometrie hat den Ruf, besonders sicher zu sein
  - Aber Fehlerraten und Konfigurierbarkeit

- Diskriminierungspotenzial
  - Verfahren funktionieren nicht mit jeder Person
  - Üblich: klappt für 1-5 % der Bevölkerung nicht
  - Und: die Verfahren funktionieren nicht in jeder Situation

- Gewöhnung:
  Fingerabdrücke für ePass = Fingerabdrücke für Fitnessstudio?

⇒ **Transparenz für Betroffene?**

⇒ **Intervenierbarkeit für Betroffene?**

Die Datenschutzsicht III

- Zwischenergebnis:
  Biometrische Verfahren haben Datenschutzrisiken


ARTIKEL-29-DATENSCHUTZGRUPPE

00720/12/DE
WP 193

Stellungnahme 3/2012
zu Entwicklungen im Bereich biometrischer Technologien

Angenommen am 27. April 2012

- Daher zu prüfen: Verhältnismäßigkeit
  - Erforderlichkeit für den Zweck
  - Effizienz zur Erfüllung des Zwecks
  - Abwägung von Beeinträchtigung der Privatsphäre und Nutzen
  - Alternativen, die die Privatsphäre weniger beeinträchtigen (z.B. RFID-Etiketten/Magnetstreifenkarten für Einlass)

Möglichkeiten für mehr Datenschutz in biometrischen Systemen I

- Aktive Mitwirkung des Betroffenen bei Datenerhebung
- Nutzung verhaltensbasierter Merkmale mit einer Wissenkomponente

- Verschlüsselung biometrischer Daten (Forschungsfeld „Biometric Encryption“: Biometrie als Code*)
- Beimischung zufälliger Informationen in einzelnen Kontexten
- Widerrufbarkeit**)
- Frühe Löschung von Rohdaten

- Ausschluss von Spoofing (Vortäuschbarkeit von Aktionen des Betroffenen)

*) http://www.ipc.on.ca/images/resources/bio-encryp.pdf

**) http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultations/Opinions2011/11-02-01_FP7_EN.pdf

Möglichkeiten für mehr Datenschutz in biometrischen Systemen II

- Speicherung unter Nutzerhoheit (z.B. Chipkarten)
- Restriktive Zugriffsbefugnisse;
  Schutz von Datenbanken mit biometrischen Daten
  (Angriffsziel, Beschlagnahmemöglichkeit)

- Sichere (revisionsfeste) Protokollierung von Eingaben/Parameteränderungen

- Transparente Gestaltung, Information des Betroffenen
- Qualitätskontrolle, z.B. durch Zertifizierungen, Evaluation, Auditierungen

Achtung: betrifft auch Umgang mit Fotos

- Mittlerweile allgemeine Verfügbarkeit von biometrischen Verfahren für Gesichtserkennung auf Fotos
- Kommend: für Videos, auch für Sprechererkennung

- Beispiel: Titelbild der Sommerakademie 2009 gemorpht aus fünf Fotos von Mitarbeiterinnen des ULD

Biometrie in eIDs – die Datenschutzsicht

Beispiel: ePass

- Seit November 2005 (1. Stufe):
  - RFID Chip
    - Datenübertragung nach ISO 14443
    - Zugriffsschutz: Basic Access Control (BAC)
  - Speicherung eines digitalen, für die automatisierte Auswertung optimierten Passbildes (JPEG)
- Seit November 2007 (2. Stufe):
  - Zusätzlich digitales Bild zweier Fingerabdrücke
  - Verbesserter Zugriffsschutz: Extended Access Control (EAC)

Der ePass ist damit Teil eines verteilten IT-Systems unter auf 191 Staaten verteilter Kontrolle.

Test in 2006: Risiken bei der Passausgabe (eigenes biom. Foto in Pass eines anderen Landes)

Betroffene europäische Länder:

GB, Deutschland, Frankreich, Italien, Schweden, Dänemark, Finnland, Estland, die Niederlande, Belgien, Spanien, Portugal, Griechenland, Slowenien, Tschechien, Polen, Österreich, Slowakei, Litauen, Lettland

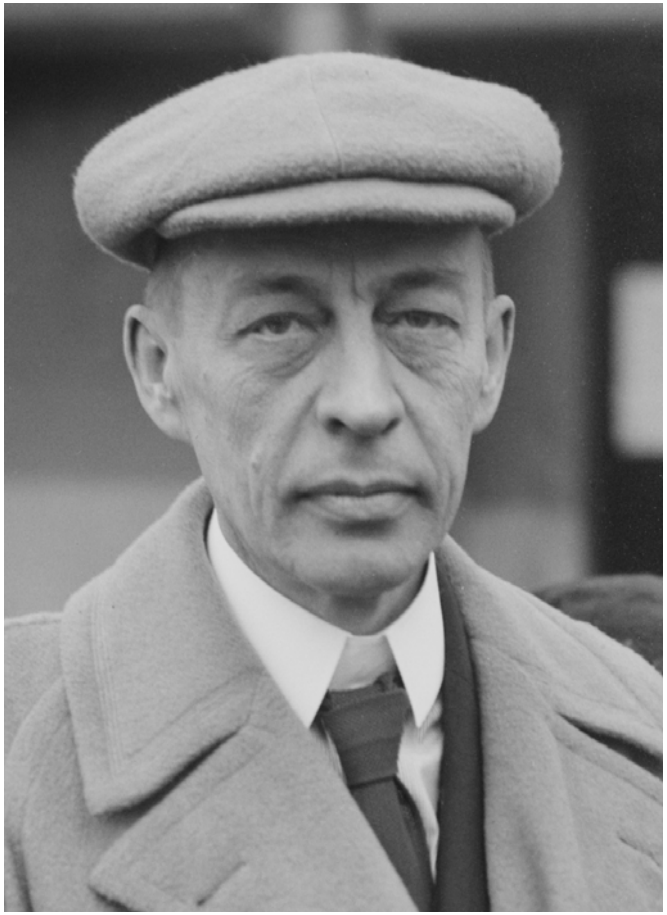
Quelle: BBC-Reportage: “My faked passport and me”,
http://news.bbc.co.uk/2/hi/programmes/panorama/6158927.stm

Datenschutzrisiken

- Generell: fehlende technische und organisatorische Absicherung der Datenschutzprinzipien, insbesondere der Zweckbindung
  - Kein Widerruf von Daten
  - Kein übergreifendes Sicherheits- und Datenschutzkonzept

- Nutzung von biometrischen Rohdaten statt Templates
  - „Kontextübergreifende Identifikatoren“
  - Verletzung der Zweckbindung („Function Creep“)
  - Verletzung des Grundsatzes der Datenvermeidung / Datensparsamkeit

Marfan-Syndrom



Sergei Rachmaninoff

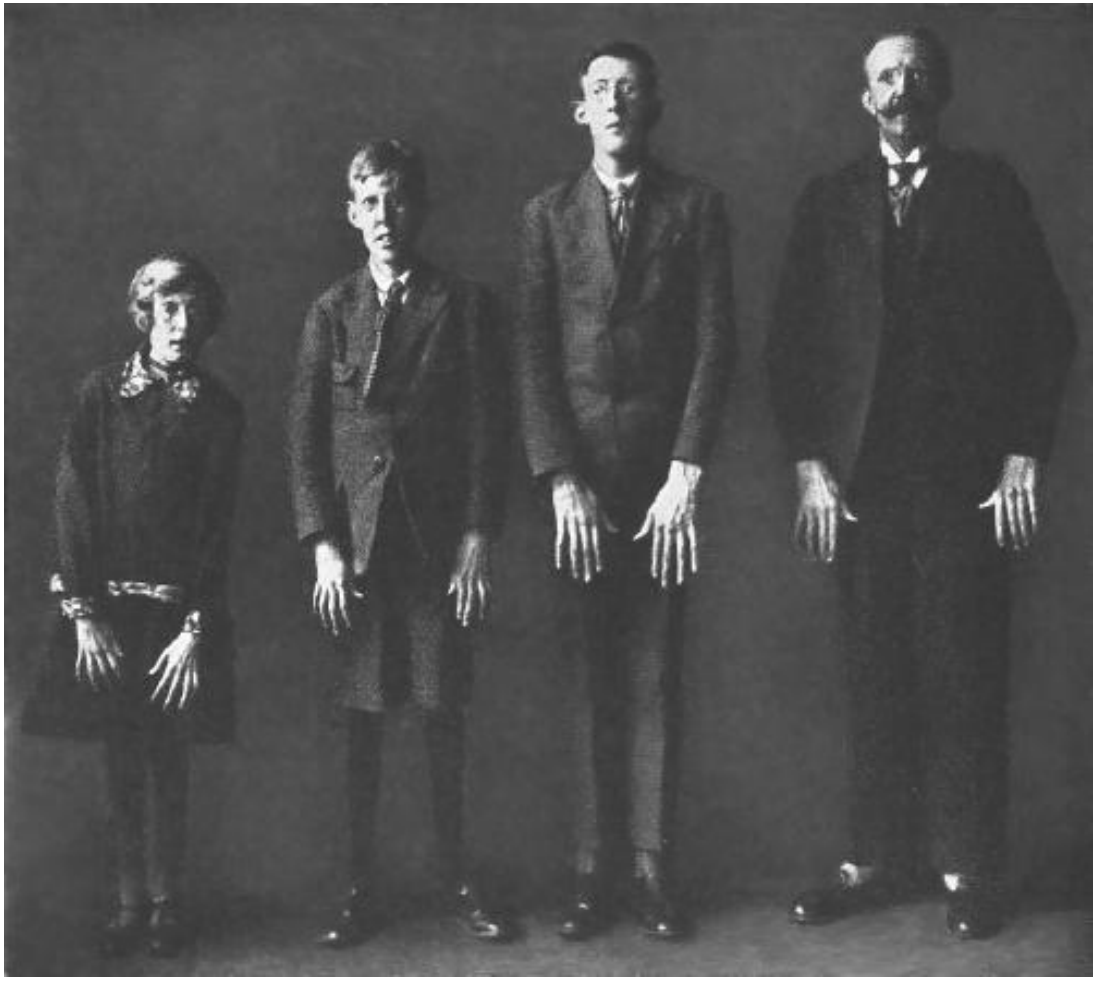


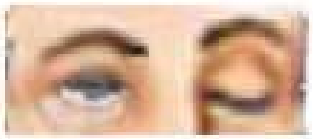
Abbildung:
Archiv f. Augenheilkunde, Band 104, 1931, S. 16; Verlag Bergmann, München

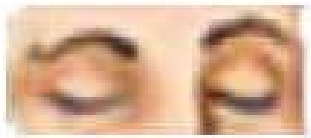
Gesichtslähmung

periphere Fazialisparese

zentrale Fazialisparese

beim Zähnezeigen und Stirnrunzeln





beim Augenschluss

Überschießende Informationen bei Gesichtsdaten

- Lebererkrankungen
  - Gelbe Färbung der Haut
- Akne
  - Pickel oder Narben
- Weitere überschießende Informationen:
  - Geschlecht
  - Augenfarbe
  - Haarfarbe
  - Ethnische Herkunft

- Automatische Analyseverfahren für solche überschießenden Informationen verfügbar
- Biometrische Optimierung des Fotos: Unterschied zu Schnappschüssen mit einer digitalen Kamera

MUSTERFOTO

► Qualitativ hochwertige Fotos sind die Grundlage einer einwandfreien Wiedergabe des Bildes und Voraussetzung für die Anwendung der Gesichtsbiometrie in Pässen.

Dieser Foto-Mustertafel sind die Qualitätsmerkmale zu entnehmen, die die Eignung der Fotos für den vorgesehenen Einsatz in Pässen gewährleisten. Es ist dringend erforderlich, die hier beschriebenen Anforderungen zu beachten, da sonst eine biometrische Erkennung des Antragstellers sowie die einwandfreie Wiedergabe des Bildes im Dokument nicht gewährleistet sind.

Der Passbewerber ist grundsätzlich ohne Kopfbedeckung abzubilden. Die Passbehörde kann vom Gebot der fehlenden Kopfbedeckung insbesondere aus religiösen Gründen, von den übrigen Anforderungen aus medizinischen Gründen, die nicht nur vorübergehender Art sind, Ausnahmen zulassen.

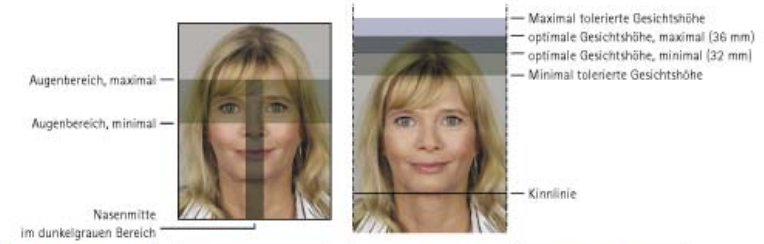
Auf den Fotos sind keine Uniformteile abzubilden. ◄

FORMAT

► Das Foto muss die Gesichtszüge der Person von der Kinnspitze bis zum oberen Kopfende, sowie die linke und rechte Gesichtshälfte deutlich zeigen. Die Gesichtshöhe muss 70 - 80 % des Fotos einnehmen. Dies entspricht einer Höhe von 32 - 36 mm von der Kinnspitze bis zum oberen Kopfende. Dabei ist das obere Kopfende unter Vernachlässigung der Frisur anzunehmen.

Wegen des häufig nicht eindeutig zu bestimmenden oberen Kopfendes sind Passfotos jedoch erst dann abzulehnen, wenn die Gesichtshöhe 27 mm unterschreitet oder 40 mm überschreitet.

Bei volumenreichem Haar sollte darauf geachtet werden, dass der Kopf (einschl. Frisur) möglichst vollständig abgebildet ist, ohne aber die Gesichtsgröße zu verkleinern. Das Gesicht muss zentriert auf dem Foto platziert sein. ◄



SCHÄRFE UND KONTRAST

► Das Gesicht muss in allen Bereichen scharf abgebildet, kontrastreich und klar sein. ◄

AUSLEUCHTUNG

► Das Gesicht muss gleichmäßig ausgeleuchtet werden. Reflexionen oder Schatten im Gesicht sowie rote Augen sind zu vermeiden. ◄

Überschießende Informationen in Fingerabdruck-Rohdaten

- Hautzustand / Hauterkrankungen
  - Ekzeme
  - Abgeriebene Papillarstrukturen (z.B. bei schwerer körperlicher Arbeit)
- Ernährungszustand der Mutter in den ersten drei Schwangerschaftsmonaten
- Empirische Studien, die Wahrscheinlichkeiten liefern
  - zur Zugehörigkeit zu einer bestimmten Rasse,
  - über geografische Herkunft oder
  - darüber, Krankheiten zu haben (darunter genetisch vererbte) oder zu entwickeln (z.B. Magenprobleme)
- Problemfeld „Handlesen“ (angebl. Kriminalität, Homosexualität)

Problemfeld „Antispoofing“

- Verfahren zur Lebenderkennung (Liveness Detection) zum Schutz vor Kopien von Merkmalscharakteristika

- Problem: Erhebung zusätzlicher und teilweise auch überschießender Daten
  - Leitfähigkeitsmessung bei Fingerkuppen (Leitfähigkeitsmessungen der Haut werden auch bei „Lügendetektoren“ eingesetzt)

Biometrie in Sozialen Netzwerken – die Datenschutzsicht

Biometrie in Sozialen Netzwerken: Quellen

Quellen für biometrische Informationen:

- Fotos (selbst- oder fremdeingestellt)
- Videos (selbst- oder fremdeingestellt)
- Chats
- Eigene Angaben zu Größe, Gewicht, Stimmung
- Daten über Apps
  - Spiele
  - Fitness
- (Verhalten)

⇒ Photo Tagging / Photo Tag Suggestions

Rockpalast

RHEINKULTUR-Festival Bonn 2011

Hilfe und Infos zur Verpixelung

Das Gigapixel-Panorama-Projekt

Der WDR-Rockpalast
(Mit vielen Infos zum Festival)

Rheinkultur 2011
(Homepage des Veranstalters)

http://rheinkulturpanorama.de/

WAS GEHT? SEARCHING...SEEK & TÄG! F.A.Q. NDR.de

NDR Wacken 2011 - Giga-Panorama

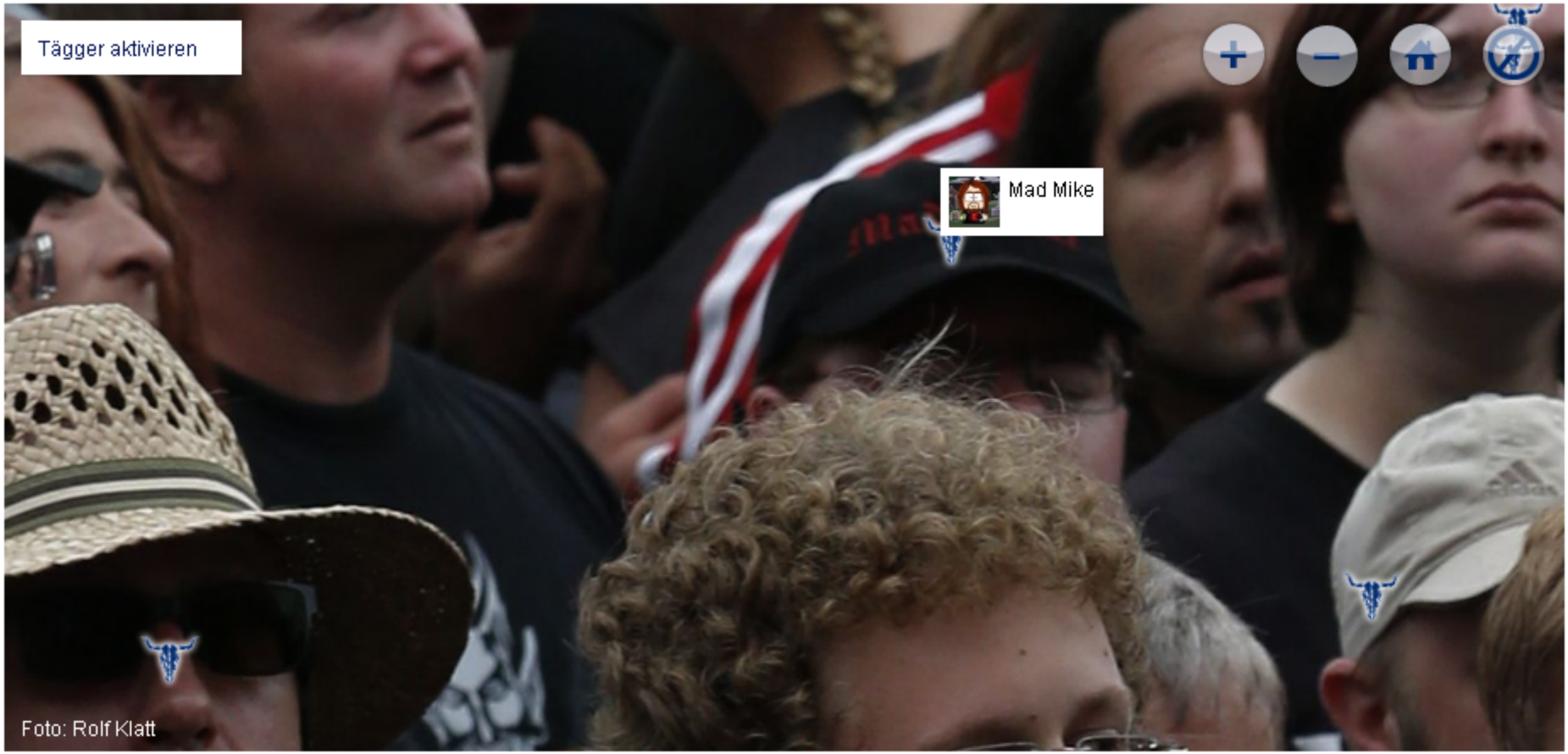
Suche und finde dich und deine Freunde auf dem NDR Wacken 2011 - Giga-Panorama.

Wenn du dich gefunden hast, tagge deine Position und poste deinen Tag auf deiner Pinnwand in Facebook oder im Buschfunkt im VZ Netzwerk.

Wacken Open Air: Metal auf der Kuhweide

Bei NDR.de bist du mittendrin im Geschehen - Bildergalerien, Livestreams und Videos, Reportagen, ein Wacken-Quiz und vieles mehr gibt es im Internet-Special zum größten Heavy-Metal-Festival der Welt unter www.ndr.de/wacken


Tägger aktivieren
Foto: Rolf Klatt


Tägger aktivieren
Mad Mike
Foto: Rolf Klatt

Die meisten getaggten Personen haben ein Profil mit echten Daten.

Facebook-Funktion Photo Tagging

https://www.facebook.com/notes/facebook-pages/feature-launch-photo-tagging-for-pages/10150168953654822

Facebook-Funktion Photo Tagging

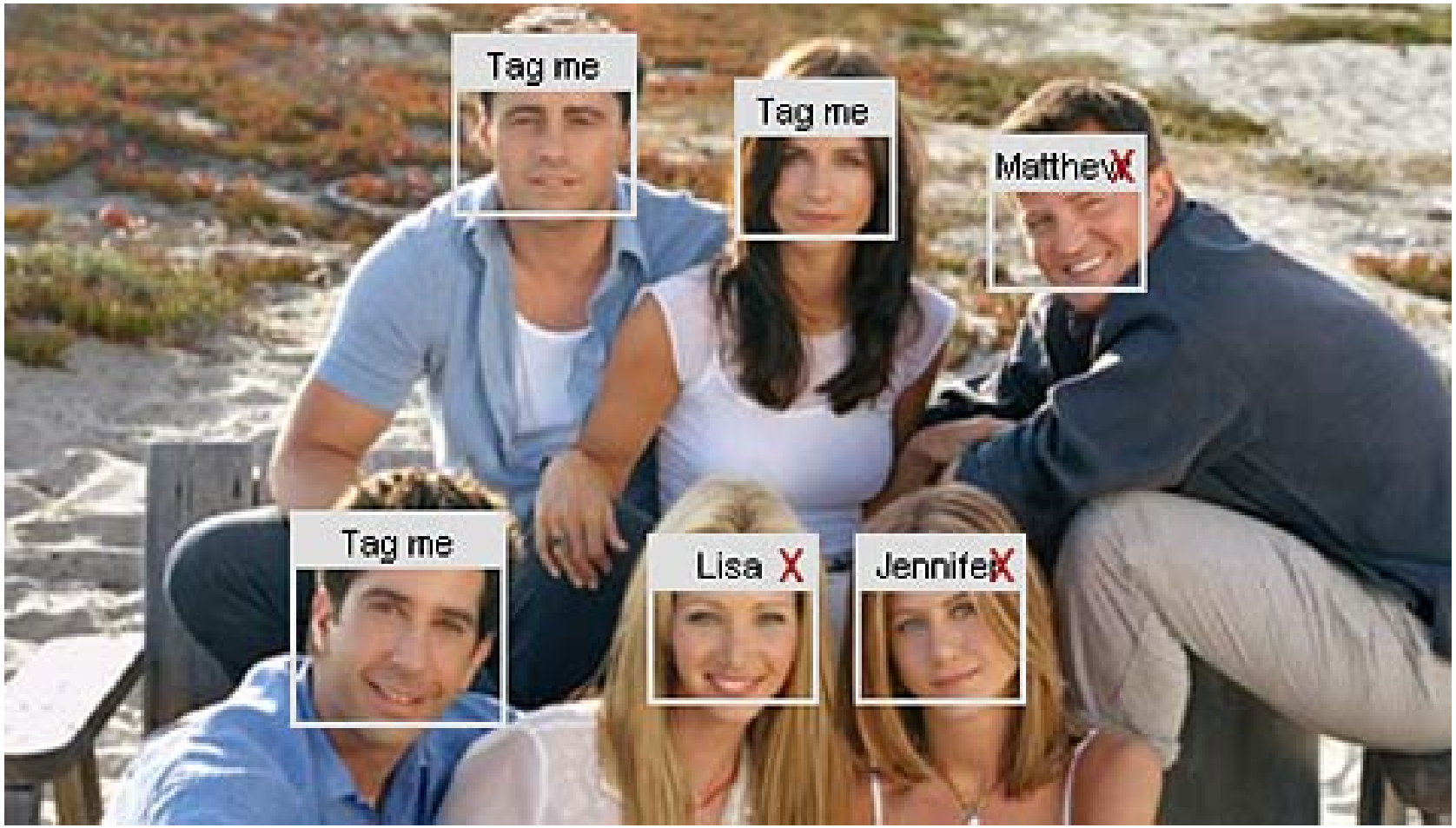


Foto: Screenshot Face.com


Gib einen Namen oder eine Markierung ein:
thomas hutter's
Thomas Hutter's Social Media Blog
Beratung/Dienstleistungsunterneh

Biometrie in Sozialen Netzwerken: Besonderheiten bei Fotos in Facebook

- Facebooks Sicht: „Einwilligung“ / Verantwortung der User
- Die Fotos sind nicht biometrisch optimiert
- Möglichkeit des Taggings auf Fotos („Wer ist das?“)
- Crowd-Ansatz „Alle helfen mit“
- Funktion „Photo Tag Suggestions“
  - Analyse der biometrischen Gesichtsdaten (bis 09/2012)
  - Ausnutzen der Wahrscheinlichkeit, dass mehrere Personen auf einem Foto auch Facebook-„Freunde“ sind
  - Ständige Korrektur durch User
  - Opt-out möglich, aber nicht gegen biometrische Analyse

Irischer Datenschutzbeauftragter, Auditbericht vom 21.12.2011

"Biometric data are not among the data categories given special protection in the Irish Data Protection Acts or in the EU Data Protection Directive. [...]

This case law [in Ireland] has not considered that the processing of biometric data requires explicit consent.

On the other hand, biometric data have been afforded special protection in the laws of certain States, and the EU's Article 29 Working Party has suggested that such a categorisation should be considered in the future EU data protection regime. We therefore recommend from a best practice perspective that FB-I take additional action."

Gesichtserkennung wird in Europa abgeschaltet und die biometrischen Daten bis zum 15. Oktober gelöscht

Teilen

Philipp Roth • 24. September 2012 News

NAUGHTYAMERICA Face Match

Upload, link, or email an image from your favorite site or mobile app

Fun. Easy. Free.

LATEST ARTICLES

September 18, 2012

Busty Schoolteacher Looks Like A Porn Star!!!

So I live right by this middle school and everyday I'm out walking by after work and I see this teacher staring at me. She's a hot thing with blonde hair, nice big tits, a big smile, and long legs, and I just had to talk to her. So I go up to her and she ignores me and blows me off like she's some kind of important model. Instantly, I knew I had to get as picture of her so I could get back at her by finding her porn star match with Naughty America's facematch tool. I wish she would have come over, but whatever; her results have made me happy time and time again.

Click here to see the busty schoolteacher's porn star look-a-like!

try it

* You must upload a JPG file. For best results, the uploaded picture should be a well lit photo with a face that is facing forward and not obscured by anything.

Upload Picture

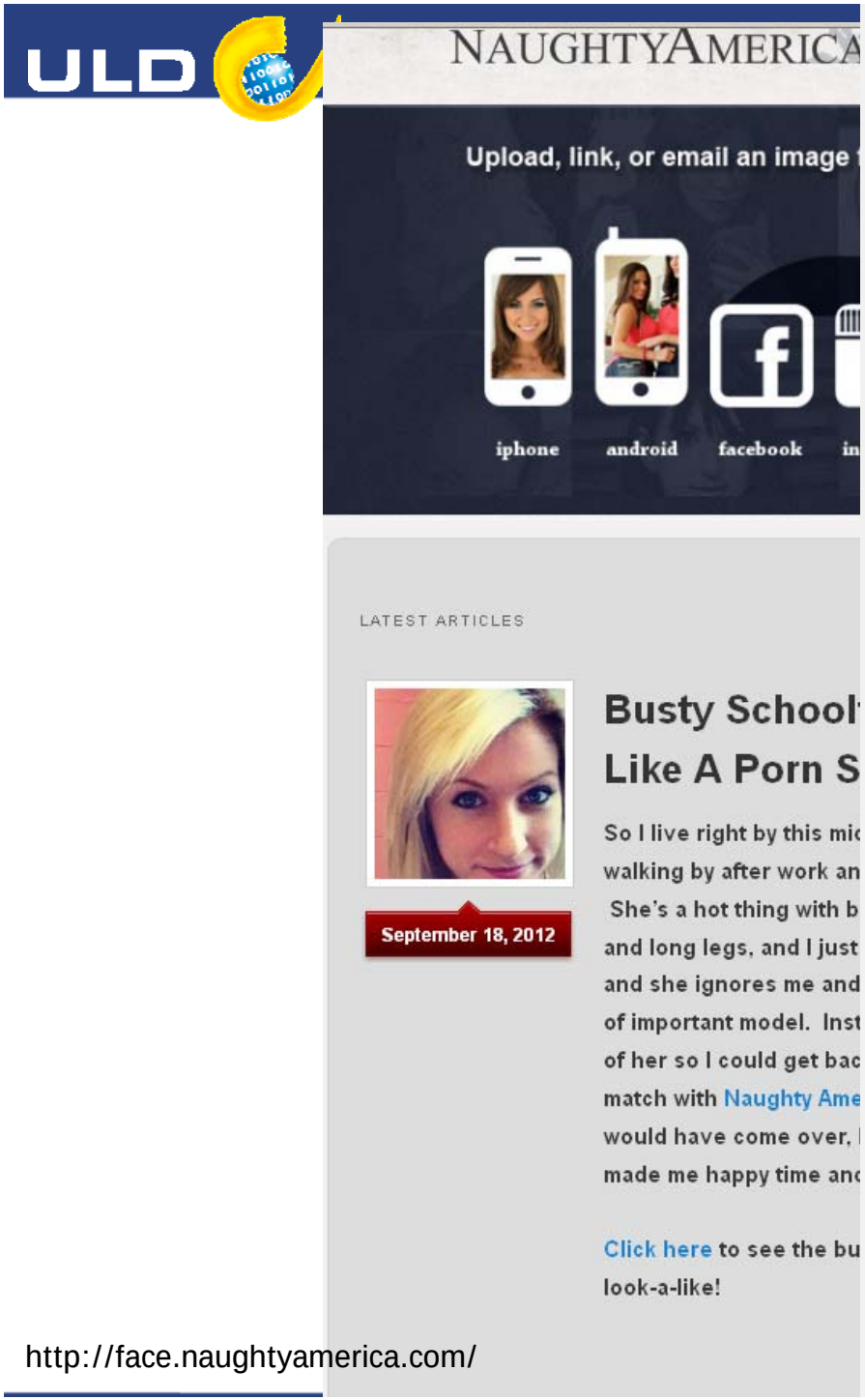
Durchsuchen...

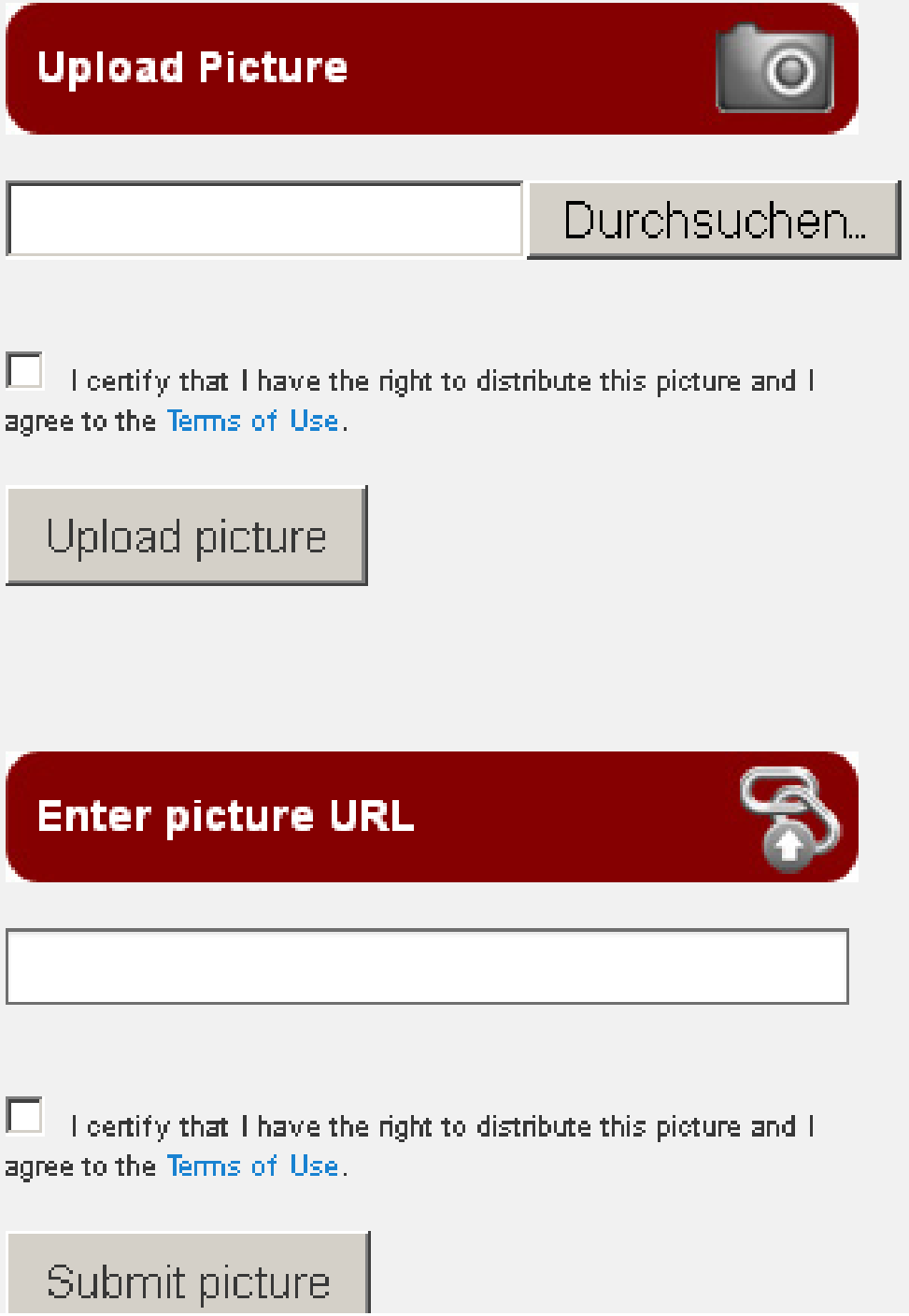
I certify that I have the right to distribute this picture and I agree to the Terms of Use.

Upload picture

Enter picture URL

http://face.naughtyamerica.com/





http://face.naughtyamerica.com/

Busty Schoolteacher Looks Like A Porn Star!!!

So I live right by this middle school and everyday I'm out walking by after work and I see this teacher staring at me. She's a hot thing with blonde hair, nice big tits, a big smile, and long legs, and I just had to talk to her. So I go up to her and she ignores me and blows me off like she's some kind of important model. Instantly, I knew I had to get as picture of her so I could get back at her by finding her porn star match with Naughty America's facematch tool. I wish she

Google auch?

Facial Recognition: The One Technology Google Is Holding Back

The Huffington Post | Bianca Bosker | First Posted: 06/01/11 09:53 AM ET | Updated: 08/01/11 06:12 AM E

SHARE THIS STORY

Google has been known for ambitiously developing technology that seems more science fiction than Silicon Valley, such as self-driving cars, but former Google CEO Eric Schmidt shared one technology he says is the only one Google has ever built, then withheld: facial recognition.

"We built that technology and we withheld it," Schmidt said of facial recognition at the All Things Digital D9 conference in California. "As far as I know, it's the only technology Google has built and, after looking at it, we decided to stop."

"I'm very concerned personally about the union of mobile tracking and face recognition," he explained, adding that the company feared that these capabilities could be used both for good and "in a very bad way." Schmidt described a scenario in which an "evil dictator" could use facial recognition to identify people in a crowd and use the technology "against" its citizens.

Google auch?

Facial Recognition: The One Technology Google Is Holding Back

The Huffington Post | Bianca Bosker | First Posted: 06/01/11 09:53 AM ET | Updated: 08/01/11 06:12 AM E

SHARE THIS STORY

Google has been known for ambitiously developing technology that seems more science fiction than Silicon Valley, such as self-driving cars, but former Eric Schmidt shared one technology he ly one Google has ever built, then l recognition.

technology and we withheld it," of facial recognition at the All Things ference in California. "As far as I know, chnology Google has built and, after ve decided to stop."

erned personally about the union of g and face recognition," he explained, e company feared that these uld be used both for good and "in a " Schmidt described a scenario in dictator" could use facial recognition to in a crowd and use the technology itizens.

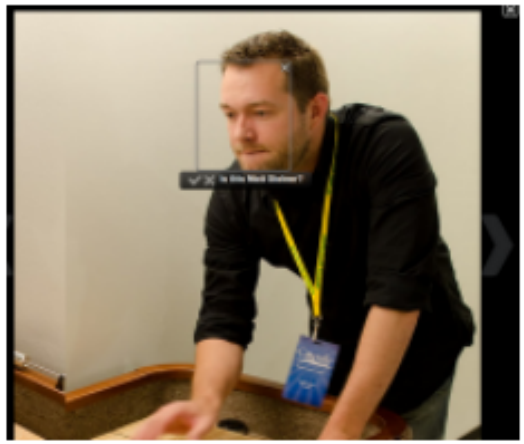
Saturday, December 10, 2011

Facial Recognition No Longer "Too Dangerous" For Google

Activist Post

Only six months after former CEO of Google, Eric Schmidt, called facial recognition software "too dangerous to implement," Google introduces the 'Find My Face' tool for Google+ users.

This week, Google made the announcement that they were rolling out facial recognition tools in a Google Plus blog post, "It is now even easier to tag photos of yourself and your friends, thanks to a new feature we are rolling out called Find My Face, which will help your friends tag your photos if you are in their pictures, and help you tag them if they have activated Find My Face."



Matt Steiner Google Engineer
Google Plus image

Biometrie in der Cloud – die Datenschutzsicht

Biometrie in der Cloud – die Datenschutzsicht

- Cloud Computing:

  Ein oder mehrere Anbieter bieten die bedarfsgerechte Nutzung von Informationstechnik (Infrastruktur, Plattform oder Software) über ein Netz an – häufig geringere Kosten als bei eigener Realisierung

- Problem des möglichen Kontrollverlusts

Studie erwartet mehr Biometrie in der Cloud bei Mobiltelefonie

Welcome | Reports | Products & Services | Company | Media Centre | White Papers | Items: 0 Total: £0.00

Home › Reports › **Mobile Phone Biometric Security - Analysis and Forecasts 2011-2015**

Report Store | My Basket | My Account

Mobile Phone Biometric Security - Analysis and Forecasts 2011-2015

Report Summary

Mobile Phone Biometric Security is a strategic analysis of the market for mobile phone biometric security products and services.

Author: Alan Goode

Publication Date: 30th June 2011

Number of Pages: 246

Enquire before you buy, email us on sales@goodeintelligence.com

£2,500.00 ADD TO BASKET

Siri: iPhone-Sprachassistenz in der Cloud

MIT Technology Review

BUSINESS REPORT The Value of Privacy

Wiping Away Your Siri "Fingerprint"

Your voice can be a biometric identifier, like your fingerprint. Does Apple really have to store it on its own servers?

By David Talbot on June 28, 2012

View full report Download

Stimm-Biometrie in der Apple-Cloud

Trudy Muller, an Apple spokeswoman, confirmed that voice recordings are stored when users ask a spoken question like “What’s the weather now?”

“This data is only used for Siri’s operation and to help Siri improve its understanding and recognition,” she said.

Muller added that the company takes privacy “very seriously,” noting that questions and responses that Siri sends over the Internet are encrypted, and that recordings of your voice are not linked to other information Apple has generated about you.

(Siri does upload your contact list, location, and list of stored songs, though, to help it respond to your requests.)

Nina: wie „Siri“ für Android und iOS

Nuance offers iOS, Android SDK for Siri-like Nina assistant

updated 12:55 pm EDT, Mon August 6, 2012

Voice assistant includes voice biometrics for security

Nuance has released a software development kit for its previously announced virtual-assistant software, named Nina (Nuance Interactive Natural Assistant). The SDK will allow developers to add voice-based features to their apps, though Nuance suggests Nina is geared for businesses that want to automate their mobile product support, rather than providing the more general appointment scheduling and message composition services offered by Siri and Google Now.

Taking advantage of N
specific phrases such
either a call to a custc
biometrics are also s
passwords.

Built-in vocal biometrics are also said to recognize the speaker, allowing the software to handle account security without passwords.

Developers can utilize the Nina Virtual Assistant SDK for both Android and iOS platforms, with initial support for US, British and Australian English—other languages are promised for later in the year. Nuance is also allowing organizations to brand their own virtual assistant persona, utilizing one from an existing range of Nuance text-to-speech voices or paying for a custom voice to be created. [via *Engadget*]

http://www.electronista.com/articles/12/08/06/voice.assistant.includes.voice.biometrics.for.security/

Risiken in (ausländischen) Clouds: unbekannte lesende / ändernde Zugriffe

- Zugriff durch Aufsichts- und Ermittlungsbehörden in Drittländern häufig ohne Information der Betroffenen
- „Indecency-Check“: Filtern/Entfernen/Blockieren von (als anstößig eingestuften) Inhalten, ggf. Account-Sperrung
- **Bei US-Anbietern auch Daten in der EU betroffen!**

Cloud-Computing: US-Behörden dürfen auf Daten europäischer Server zugreifen

von Kai Schmerer und Zack Whittaker, 1. Juli 2011, 11:21 Uhr

Themenseiten

Cloud-Computing, E-Mail, Kommunikation, Google, Microsoft, Wikileaks

Mehr zum Thema

- Fehlermeldungen zu Office 365 häufen sich vor Launchtermin
- "Wikileaks und Amazon haben Cloud Computing einen Bärendienst erwiesen"
- Bericht: Amazon verbannt Wikileaks von seinen Servern
- US-Kongressabgeordne "Wikileaks ist eine Terrororganisation"

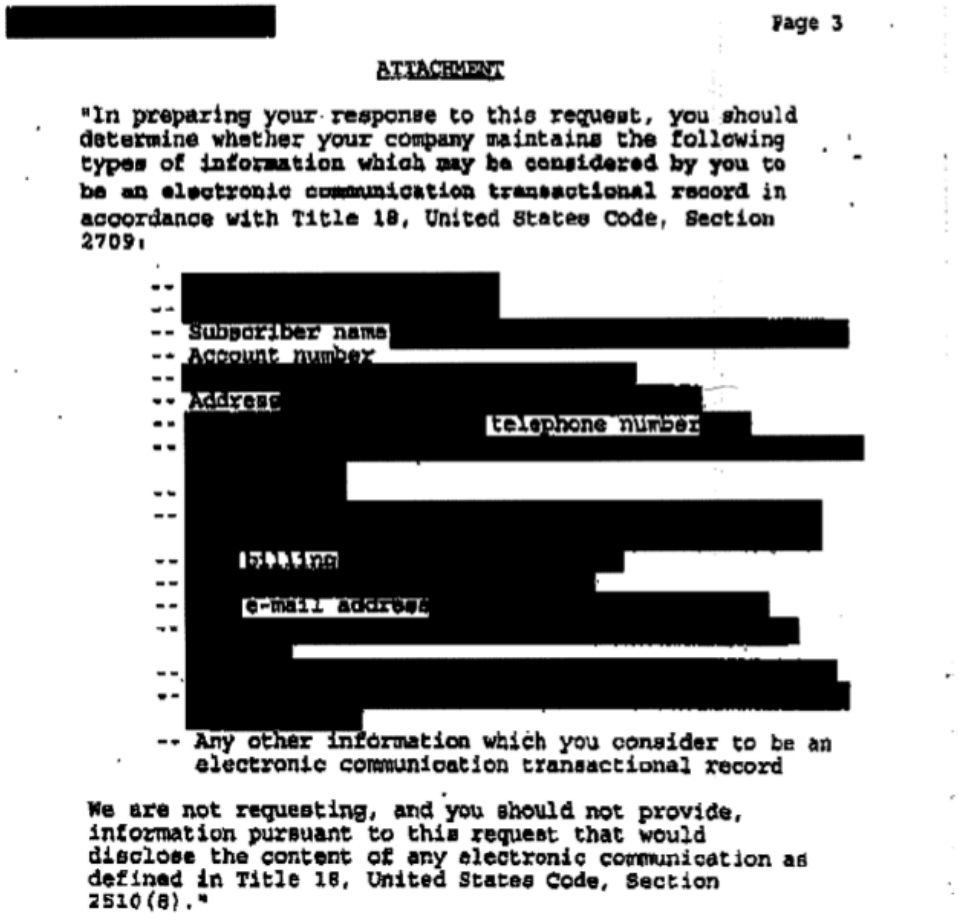
Der Geschäftsführer von Microsoft UK Gordon Frazer hat im Rahmen einer Pressekonferenz zu Office 365 in London bestätigt, dass US-Behörden auf Daten europäischer Server zugreifen dürfen, die von einem US-Unternehmen betrieben werden. Dies betreffe alle Firmen mit Hauptsitz in den USA. Grundlage hierfür ist das amerikanische Antiterrorgesetz USA Patriot Act.

Auf die Frage eines Journalisten, ob Microsoft den Schutz von Daten auf europäischen Servern garantieren könne, wenn US-Behörden mit dem Verweis auf den Patriot Act darauf zugreifen wollen, antwortete Frazer: "Microsoft kann diese Garantien nicht geben. Kein US-Unternehmen kann das." Sofern es gesetzlich möglich sei, werde man betroffene Kunden über den Zugriff von US-Behörden informieren.

Über den Umgang mit Daten hat Microsoft ein Whitepaper veröffentlicht, das die Aussagen von Frazer weiter präzisiert. In dem Online-Dokument "Data Use Limits" ist in Sachen Datenweitergabe nicht nur im Zusammenhang mit dem Patriot Act die Rede. Dort steht, dass generell "rechtliche Anforderungen" die Weitergabe von Daten notwendig machen könnten.

Nicht nur der Patriot Act

- In den USA auch **Beschlagnahme** von Daten **rechtlich möglich** bei:
  - „Bank of Nova Scotia Subpoena“
  - „Compelled Consent Order“ (insbes. für Bankdaten)
  - Foreign Intelligence Surveillance Act (u.a. Sec. 1881a FISA)
  - National Security Letters vom FBI (ohne richterlicher Beschluss)



[redacted] Page 3

ATTACHMENT

"In preparing your response to this request, you should determine whether your company maintains the following types of information which may be considered by you to be an electronic communication transactional record in accordance with Title 18, United States Code, Section 2709:

-- [redacted]
-- Subscriber name [redacted]
-- Account number
-- [redacted]
-- Address
-- [redacted] telephone number [redacted]
-- [redacted]
-- [redacted]
-- [redacted]
-- [redacted]
-- e-mail address
-- [redacted]
-- [redacted]
-- [redacted]
-- Any other information which you consider to be an electronic communication transactional record

We are not requesting, and you should not provide, information pursuant to this request that would disclose the content of any electronic communication as defined in Title 18, United States Code, Section 2510(8)."

http://scr3.golem.de/screenshots/1011/nsl/nsl.png

Mögliche Zugriffe nicht nur von den USA

Außereuropäische Beispiele:

- Algerien
- Bahrain
- China
- Indien
- Indonesien
- Iran
- Libanon
- Pakistan
- Russland
- Saudi-Arabien
- Vereinigte Arabische Emirate
- ...

Innereuropäisch von Bedeutung:

- RIPA (Großbritannien)
- FRA-Lagen (Schweden)

Problem bei Auslands-Clouds: Filtern/Entfernen/ Blockieren von Daten/Accounts vorbehalten

AGBs lesen!

Terms of Service Agreement

3.2. **User Files.** You may be permitted to upload executable files or other content to the CloudXYZ Servers in various forms (collectively, "User Files"). By providing any User Files, you agree that it will not: (i) infringe any copyright, trademark, patent, trade secret, or other proprietary right of any party; (ii) be profane, obscene, indecent or violate any law or regulation; (iii) defame, abuse, harass, threaten or otherwise violate the legal rights (such as rights of privacy and publicity) of others; (iv) incite discrimination, hate or violence towards one person or a group because of their belonging to a race, a religion or a nation, or that insults the victims of crimes against humanity by contesting the existence of those crimes; or (v) restrict or inhibit any other user from using the CloudXYZ Service. We have no obligation to monitor User Files related to the CloudXYZ Service. However, we reserve the right to review User Files and take any action we deem necessary as to such User Files, including but not limited to editing or removing your User Files and/or suspending or terminating your access to CloudXYZ based on your violation of the rules specified here.

Problem bei Auslands-Clouds: Filtern/Entfernen/Blockieren von Daten/Accounts vorbehalten

Terms of Service Agreement

3.2. **User Files.** You may be permitted to upload executable files or other content to the CloudXYZ Servers in various forms (collectively, "User Files"). By providing any User Files, you agree that it will not: (i) infringe any copyright, trademark, patent, trade secret, or other proprietary right of any party; (ii) be profane, obscene, indecent or violate any law or regulation; (iii) defame, abuse, harass, threaten or otherwise violate the legal rights (such as rights of privacy and publicity) of others; (iv) incite discrimination, hate or violence towards one person or a group because of their belonging to a race, a religion or a nation, or that insults the victims of crimes against humanity by contesting the existence of those crimes; or (v) restrict or inhibit any other user from using the CloudXYZ Service. We have no obligation to monitor User Files related to the CloudXYZ Service. However, we reserve the right to review User Files and take any action we deem necessary as to such User Files, including but not limited to editing or removing your User Files and/or suspending or terminating your access to CloudXYZ based on your violation of the rules specified here.

AGBs lesen!

User Files, you agree that it will not: (i) infringe any copyright, trademark / party; (ii) be profane, obscene, indecent or violate any law or regulation;

reserve the right to review User Files and take any action we deem necessary as to such User Files, editing or removing your User Files and/or suspending or terminating your access to CloudXYZ base

Problem bei Auslands-Clouds: Filtern/Entfernen/Blockieren von Daten/Accounts vorbehalten

AZ-WEB.DE Aachener Zeitung

Wie ein Handy-Fan von Wolke Sieben fiel

Von Marc Heckert | 01.02.2011, 08:00

Aachen. Von seinem brandneuen Windows Phone war Dirk Salm begeistert. Vor allem die Verknüpfung des Edel-Handys mit Programmen und Funktionen im Internet faszinierte den Aachener Fotografen. Bis ihm in der vergangenen Woche der Zugang zu diesen Web-Inhalten gesperrt und mit Kontokündigung gedroht wurde.

Zu seinem Erstaunen erfuhr Salm, dass einige seiner Bilder gegen Microsofts Geschäftsbedingungen verstoßen hätten. Nun wundert sich der 42-Jährige, dass seine Daten, die er für privat hielt, anscheinend durchleuchtet wurden. «Was ist mit Datenschutz?», fragt er.

Weitere Entwicklungen

Miniaturisierung bei Audio und Video

Nicht nur
aus China:

Lanmda Technology Co., Ltd (China)

Kopplung von Minikameras mit Biometrie

Beispielsweise in Schaufensterpuppen

Quelle: http://www.almax-italy.com/

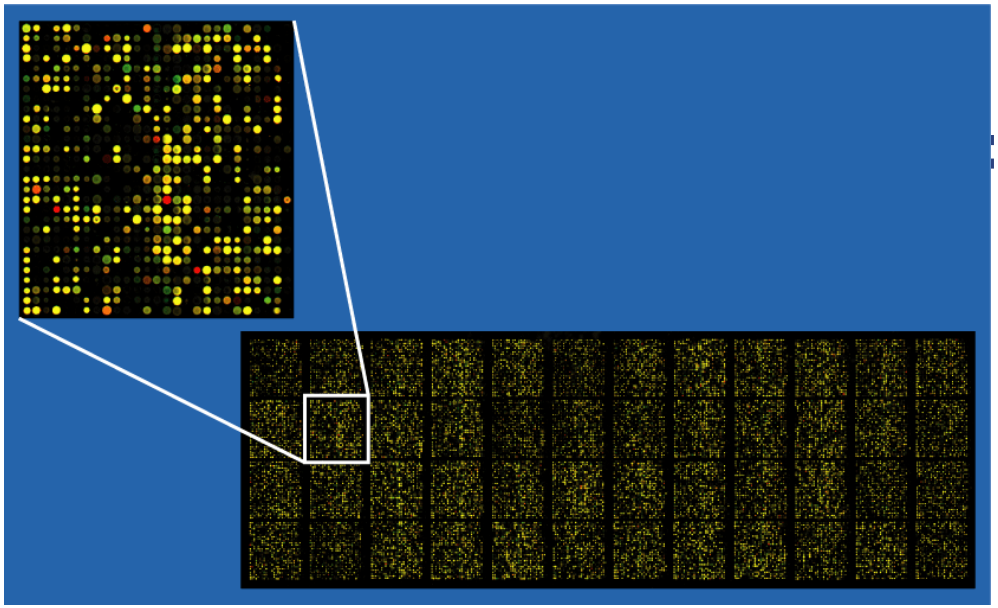
Apple-Patent zum Diebstahlschutz: via iPhone (Aug. 2010)

- „Systeme und Verfahren zum Identifizieren nicht-autorisierter User eines elektronischen Geräts“
- Identitätsprüfung per Foto, Stimme, Herzschlag, ...
- Läuft stets im Hintergrund mit

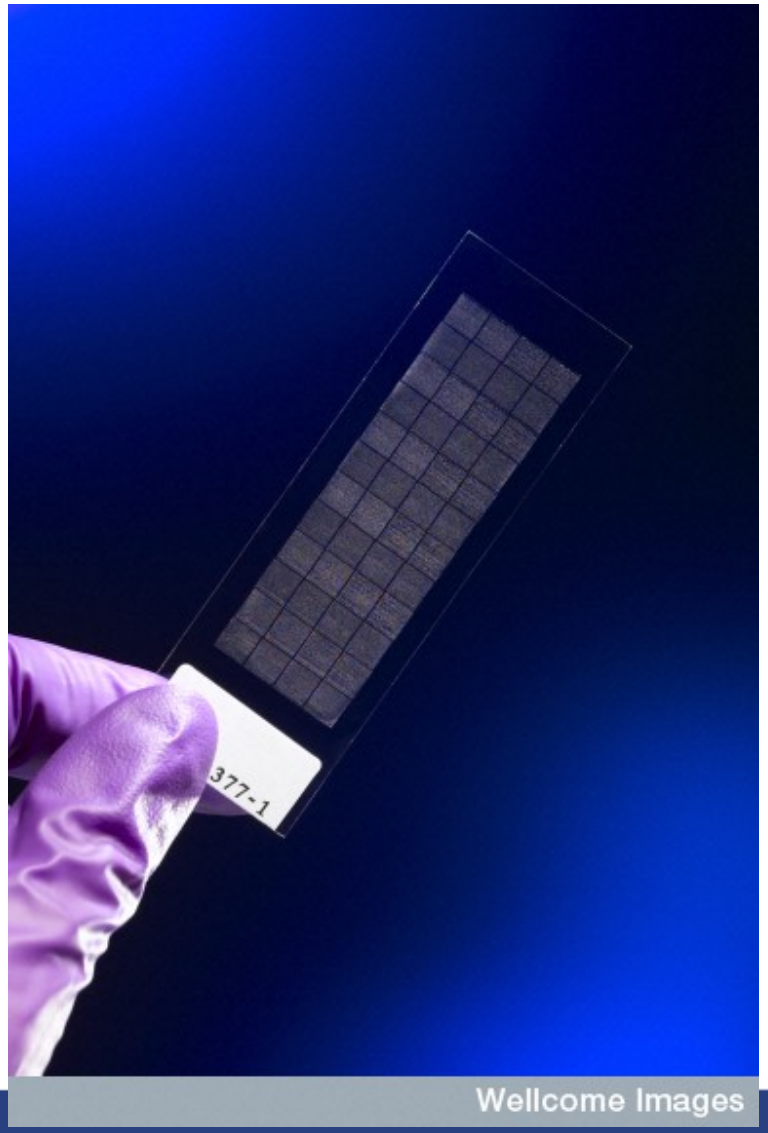
⇒ Viele Datenschutzfragen!

- Alles unter Kontrolle von Apple?

Verwandt: Genanalyse



- Analyse von ~100.000 Genen per DNA-Chip



Wellcome Library, London

Fazit

Fazit

- Biometrie ist ein Datenschutz-Risiko

- Die seit Jahrzehnten diskutierten Risiken verschärfen sich
  - ... bei eIDs in der heutigen Gestaltung (Rohdaten statt Templates, teilweise zentrale Datenbanken)
  - ... in Sozialen Netzwerken (besonders Fotoanalyse)
  - ... durch Cloud Computing (Kontrollverlust; Verschlüsselung oft keine Lösung)

- Gesellschaftliche Betrachtung von Biometrie im Bereich Sicherheit und Grenzen muss die Entwicklungen in Sozialen Netzwerken und Clouds einbeziehen