EAB Newsletter
Edition April 2014

Editors: Christian Rathgeb, Max Snijder
Contact: secretariat@eab.org

Production:
This newsletter is issued by the European Association for Biometrics (EAB). Its content is contributed by the members of the EAB. If you feel an important news from your biometric sector or from your Region missing – do not hesitate to submit a news item to the secretariat before the next newsletter is issued (July 2014).
1. **News from the EAB**
   - EAB signs long term agreement with Mesago on Euro ID and ID World International Congress
   - Welcome to the latest 10 EAB members!
   - EAB to organize special seminar on biometrics for financial transactions, hosted by the Association of German Banks
   - Bernard Didier elected as the first Honorary Member of the European Association for Biometrics
   - European Association for Biometrics (EAB) organizes largest European research conference on biometrics

2. **EU/EC/EP**
   - 3D Face technology reveals genetic and other disorders
   - EDPS calls Germany to take the lead in negotiating the EU DP Regulation
   - Court decisions and other legal issues
   - EU DPAs and APEC take a step towards mutual recognition of BCR/CBPR
   - France's CNIL fines Google 150,000 euros for non-compliant privacy policy
   - Make-up and fake fingers – staying ahead of the online spoofer
   - Snowden Testimony for European Parliament
   - UBIN launches USB biometric enterprise security device

3. **Outside Europe**
   - International Standardisation now active for more than 10 years
   - FICV: a new FVCongoing benchmark area on Face Compliance Verification to ISO/IEC 19794-5:2011
   - How to Apply International Human Rights Law to NSA Spying

4. **Industry**
   - Apple publishes whitepaper on iOS security, details Touch ID fingerprint sensor specs, functionality
   - Frost and Sullivan – Biometrics in cell phones
   - IDEX and CrucialTec partner up for mobile touch sensors
   - Cognitec Algorithm Receives Best Rating in NIST Independent Vendor Test
   - The Swiss Center for Biometrics Research and Testing is born!

5. **Events**
   - EAB seminar on biometrics for financial transactions, Berlin May 21: special rates for EAB members
   - European Biometrics Research and Industry Awards 2014: call for candidates
   - EAB Research Projects Conference (EAB-RPC) 2014, Darmstadt 8-9 September 2014
   - International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt 10-12 September 2014 – Call for Papers
   - ID World International Congress - Call for Papers, 18-20 November 2014
   - International Joint Conference on Biometrics - IJCB’14, Clearwater Beach, USA 29 September – 2 October

6. **Reports**
   - European Standardisation in CEN
   - 1st International Symposium on 3D Face Recognition Twente
   - NBL Annual Workshop 2014
   - German Biometrics Working Group Meeting
   - NIST International Biometric Performance Conference – IBPC-2014
   - NIST EAB Session on Biometric Ageing at the IBPC-2014
   - EAB Workshop on Forensics and Biometrics 2014

7. **Impressum**
1. News from the EAB

EAB signs long term agreement with Mesago on Euro ID and ID World International Congress

March 2014 - The European Association for Biometrics (EAB) and Mesago Messe Frankfurt GmbH, the organizer of the Euro ID and ID World International Congress, have entered into a long term cooperation that aims at creating a platform on biometrics and identity within the event. In addition parties have agreed upon a mutual marketing and communication agreement that will significantly increase the outreach and coverage of mutual communication channels.

Max Snijder, Secretary of the EAB, says:

“We are happy that Mesago has selected EAB as a strong partner to further develop this major event by bringing in the largest network on biometrics and identity in Europe. Together with Mesago we will bring the topic of biometrics towards specific vertical market segments, broadening the scope of identity with the various aspects of biometrics. Events like Euro ID and ID World International Congress will further leverage the EAB’s impressive network, that spans from state of the art European academic researchers to governments and industries.”

The joined events Euro ID and ID World International Congress are the key events on identity in Europe. Frankfurt is the perfect home to join efforts thanks to its central location, great facilities and its long history of world leading events. Part of the EAB-Mesago agreement is the establishment of a Biometrics Pavilion at the exhibition, which will function as a one-stop-shopping for anyone having an interest in biometrics.

Maren Wiedleroither, Vice President of Mesago Messe Frankfurt GmbH says about the cooperation with the EAB:

“We are impressed by the rapid growth and high quality of the EAB members base. Together with the EAB we will ensure biometrics to be an integral part of the portfolio of Euro ID and ID World International Congress. Through the Biometrics Pavilion our visitors will be able to get a full picture of the state of the art in biometrics, while we also offer small and medium biometric enterprises to receive strong exposure at a cost effective way.”

About Mesago:
Mesago Messe Frankfurt, founded in 1982 and located in Stuttgart, specializes in exhibitions and conferences on various topics of technology. The company belongs to the network of Messe Frankfurt. Mesago operates internationally and is not tied to a specific venue. With
some 100 members of staff Mesago organizes events for the benefit of more than 2,700 exhibitors and over 100,000 trade visitors, conference delegates and speakers from all over the world. Numerous trade associations, publishing houses, scientific institutes and universities work with Mesago closely as advisers, co-organizers and partners.

Welcome to the latest 10 EAB members!
The EAB is still going strong and is happy to welcome its latest 10 new members:

Behaviosec (Germany, [www.behaviosec.com](http://www.behaviosec.com))
Vlatacom (Rep. of Serbia, [www.vlatacom.com](http://www.vlatacom.com))
Identity Assurance Systems (United Kingdom, [www.idassys.com](http://www.idassys.com))
University of Houston (USA, [www.uh.edu](http://www.uh.edu))
Thales (France, [www.thalesgroup.com](http://www.thalesgroup.com))
Softpro (Germany, [www.softpro.de](http://www.softpro.de))
National Bureau of Investigation (Sweden, [www.polisen.se/en](http://www.polisen.se/en))
MTRIX (Germany, [www.mtrix.de](http://www.mtrix.de))
Fingerprint Cards (Sweden, [www.fingerprints.com](http://www.fingerprints.com))
Waarith Consulting (Nigeria, [info@waarith.com](mailto:info@waarith.com))

EAB to organize special seminar on biometrics for financial transactions, hosted by the Association of German Banks

The European Association for Biometrics has opened the registration for its seminar ‘Benefits of Biometrics for Banking’. The event, which is one in a series of EAB events targeting specific application areas, will familiarize you with biometric applications can support in optimizing the following key aspects of banking process:

- Customer Interaction
- Operational Efficiency
- Fraud Prevention

Various key speakers will reflect the many new opportunities arising from the gradual shift away from desktop/notebook computing on smartphones and tablets and share best practice of apps and web-based applications. Participants will:

- hear about Biometrics solutions for in-branch and mobile usage for internal and customer-facing usage
- learn how Biometrics support mega trends such as personalization, etc.
- identify, where biometrics can be embedded into banking and other financial processes
- discuss the impact of Biometrics for the mobile payment world

Among the speakers are Waldemar Grudzien (BdB director and EAB Advisory Council member), Oliver von Treuenfels (Dermalog), Rui Wang (CEO Techshino Europe), Jens Peterson (First Attribute), Christiane Kaplan (Softpro), Peter Jones (Hitachi Europe Limited), Andreas Ewig (DSGV) and Andreas Bongers (GFT).

Waldemar Grutzien, director of the Association of German Banks, says:
"We are very happy to cooperate with the EAB to establish this seminar. There is a lot of dynamics around biometrics in the financial sector. Biometrics in smart phones really changes the paradigm, which will not leave the financial sector unaffected. With this workshop we would like to take away lessons learned and best practices in order to provide new input for our branch on the development of biometrics enabled services."

For more details on the event and registration for the event please visit the EAB website at:
http://eab.org/events/program/66

Bernard Didier elected as the first Honorary Member of the European Association for Biometrics

On 12 February 2014 the General Assembly of the European Association for Biometrics unanimously elected Dr. Bernard Didier as the first Honorary Member of The Association.

Mr. Didier, who recently retired from his long and highly successful employment with Morpho (Safran), has significantly contributed to the development of biometrics in Europe and globally. Under his leadership Morpho, which Mr. Didier founded in 1982, has grown to one of the undisputed market leaders in the global market of biometrics and identity. He not only promoted the continuous innovation in biometric technologies, but he also has contributed to the adoption of responsible practices in the use of biometrics by actively supporting Privacy by Design and sophisticated encryption technologies. About the proliferation of biometrics Mr. Didier said the following:

"Like any technology, the use of biometrics is not intrinsically good or bad; the real challenge is to strike a balance between freedom and security. It's the role of governments and personal rights organizations to set up regulations allowing governments and business to use this technology correctly."

In Europe Mr. Didier has consistently made sure Morpho participated and invested in European research on the development and deployment of biometric technologies and applications. With that, and with his consistent support of the EAB, Mr. Didier has significantly contributed to the growth of biometrics in Europe.

Bernard Didier, intervening at many conferences, radio and television broadcasts on biometrics and security, is internationally recognized as one of the leaders in the field of biometrics and received at the time of the 5th international ID WORLD congress, organized in Milan on November 28, 2006, the ID Trail Blazer Award during the evening of the ID People Awards – the Oscars of the auto ID industry –. In 2010 Bernard DIDIER received the badges of Chevalier of the Legion of Honour. That year he also was a Marius-Lavet prize-winner.

Alexander Nouak, Chair of the EAB says:

"We are happy and honoured that Mr. Didier accepted our nomination to become the EAB's first Honorary Member. For us it is an important encouragement to proceed with building a strong and competitive biometrics industry in Europe, taking into account that this technology should be deployed at a responsible manner. The EAB, now counting almost 130 members within its short
existence, can only hope that more honorary members of the level of Mr. Didier can be added to our Hall of Fame.”

European Association for Biometrics (EAB) organizes largest European research conference on biometrics

On September 8-9, 2014 Europe’s largest conference on European Commission funded research on biometrics and identity management will take place at the premises of Fraunhofer IGD in Darmstadt, Germany. The EAB-Research Project Conference 2014 will be co-located with the IEEE BIOSIG conference that will take place later that same week.

The EAB and the EU-projects FIDELITY, FastPass, BEAT, FutureID and INGRESS, are jointly organizing the EAB Research Project Conference (EAB-RPC), to present research results and in order to discuss the benefit of this research for our European society. Moreover, experts from the biometric community will discuss on a panel Ethical and Privacy Issues of Biometrics and Identity Management. Furthermore, a second panel will be devoted to discuss and identify future research topics in the Horizon2020 research program.

Christoph Busch, board member of the EAB and initiator of the conference, says:

"Biometrics and Identity Management are key research topics that are currently investigated in a number EU-projects running under the seventh Framework program. International research is dealing with innovative solutions for secure and privacy compliant biometrics and federated identity management. For the first time all major European research projects in the area of Biometrics and Identity Management are being provided a single platform for information exchange and discussion. This will contribute to a stronger research community at European level and a stronger position for European R&D in international context.”

For more details on the European Research Conference and registration for the event please visit the EAB website at: http://eab.org/events/program/69
2. EU/EC/EP

3D Face technology reveals genetic and other disorders

Back in 2008 Peter Hammond from the Institute of Child Health in London wrote the article ‘What’s in a Face?’, describing how 3D face technology is able to analyze 3D facial images to detect all kinds of syndromes and disorders. Today a medical researcher at the Amsterdam Medical Center (AMC) confirms these findings by stating that the face (especially the 3D representation of it) can show much more than we may expect. Saskia Hopman confirms that a subtle change in a single gene can have a significant influence on a person’s facial appearance. The consequences can be clear (e.g. the Down Syndrome) or more delicate (like the Marfan Syndrome). But these recognizable features go beyond just syndromes. They may also reveal disorders that involve behavior. Hammond and Hennekam published in the scientific journal Brain a thesis that describes facial characteristics of people who suffer from epileptic disorders. 5% of the epileptic disorders have a genetic cause, which cause specific features in the faces of these patients. The research that Hopman performed in the AMC proved that specific features (pronounced noses, high foreheads, long chins etc.) were easily detectable and classifiable. The 3D face technology is even being used to look for indications which genes should be more focused on in order to find a specific disorder. A research project amongst 1000 children with cancer revealed that 4% of them had a specific syndrome, which was detectable through 3D face technology.

Source: Van Elzakker, AMC Magazine 2013


Average profile and portrait of Williams syndrome (left), control (centre) and Noonan syndrome (right).

http://www.hospitalmanagement.net/features/feature1767/feature1767-2.html
EDPS calls Germany to take the lead in negotiating the EU DP Regulation

The European Data Protection Supervisor, Peter Hustinx, has urged the German government to take the lead in trying to ensure that the EU DP reform takes place before the elections of the European Parliament and Commission in May this year.

Speaking in Bonn, Germany on 13 January, Hustinx said: “Germany claims a special responsibility and role in the area of data protection. The new German government can tackle this subject with the necessary drive and energy and thereby gain acceptance of the German position at European level and lead Europe to a higher level of data protection. However, this will require a constructive and proactive approach in the European debate.”

This surprise statement reflects the frustration many feel about the lack of progress with this legislative package due to resistance by both Germany and the UK, albeit for different reasons. The next important steps was the meeting of the EU justice ministers 7-8 March 2014, and a plenary vote in the European Parliament due to take place this spring.

Hustinx praised the Parliament for preparing its compromise position last October, but said: “Unfortunately, there has been no comparable progress in the Council. Some Member States are still causing delays through general reservations.”

Vice President of the European Commission, Viviane Reding, said on 7 January: "The Heads of State and Government committed to a ‘timely’ adoption of the new rules in October. Not much progress has been made since. But I hope that under the Greek presidency that has just started, Member States will now finally take the big decisions needed. The Commission will support the Greek government's ambitious objective to reach an agreement by the summer.”

Hustinx made his remarks at the Fourth Bonn 'Regulation Meeting', 13 January 2014, at the Center for European Integration Studies (ZEI), Bonn.

Court decisions and other legal issues

European Court of Justice decided recently about the collection and storage of fingerprints for ePassports: ECJ, C-291/12 Michael Schwarz v Stadt Bochum, 17 October 2013

A German citizen, mr. Schwarz, applied for an ePassport but refused to provide his fingerprints. As a result, mr. Schwarz could not obtain an ePassport. He started court
proceedings in Germany against this refusal to provide him with an ePassport, arguing that the Regulation No 2252/2004 was invalid. In this context, the German court asked the European Court of Justice (ECJ) a preliminary question about the validity of Article 1(2) of the aforementioned Regulation. Article 1(2) requires that passports and travel documents “shall include a highly secure storage medium which shall contain a facial image. Member States shall also include two fingerprints taken flat in interoperable formats. (...)

Several aspects of the judgement of the ECJ are interesting. Some are briefly mentioned hereunder.

The Court stated that the capture and storage of fingerprints for the ePassports as mandated by Regulation No 2252/2004 on standards for security features and biometrics in passports and travel documents “constitutes (sic) a threat to the rights to respect for private life and the protection of personal data” (§30). It considers it a ‘twofold’ threat, for which a justification is needed.

The fundamental rights of privacy and data protection are indeed not absolute, and therefore interference is possible, but only under strict conditions. These conditions, states the Court, are outlined in Article 52(1) of the Charter, allowing for limitations of the exercise of those rights, so long as those limitations are provided for by law, respect the essence of those rights, and, in accordance with the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

This hence includes the need for a legitimate aim for the interference. The ECJ referred to the general interest objective of preventing illegal entry into the EU. It found that the collection and storage measures "are appropriate for attaining the aims pursued by that regulation and, by extension, the objective of preventing illegal entry to the European Union" (§45). The ECJ further found that the collection and storage of the fingerprints on the passport chip and hence the interference is “justified by its aim of protecting against the fraudulent use of passports” (§64).

Interesting for the national debate in several EU Member States is also the statement of the ECJ that the Regulation No 2252/2004 “cannot in and of itself (...) be interpreted as providing a legal basis for the centralized storage of data collected thereunder or for the use of such data for purposes other than that of preventing illegal entry into the European Union.” (§61). The Court concluded that its examination of the question submitted did not lead to elements capable of affecting the validity of Article 1(2) of Regulation No 2252/2004. For more information, you can contact els.kindt@law.leuven.be, EAB member.

EU DPAs and APEC take a step towards mutual recognition of BCR/CBPR

The EU Data Protection Authorities and the Asia-Pacific Economic Cooperation (APEC) economies have issued a checklist on the requirements that companies need to consider when applying for authorization of Binding corporate Rules (BCR) and/or certification of
APEC's Cross-border Privacy Rules (CBPR). The document will serve as an informal pragmatic checklist for organizations, and will facilitate the design and adoption of personal data protection policies compliant with each of the systems, the two bodies say.

The document, prepared jointly by APEC officials and the EU Art. 29 Data Protection Working Party, shows that there is considerable overlap between the two systems. Companies cannot achieve mutual recognition of both systems just by taking on-board the suggestions in this document, but it could serve as a basis for double certification.

The document was endorsed by APEC Senior Officials at their meeting of 27-28 February 2014, and the EU Data Protection Working Party adopted an opinion/working document on 26 February 2014.


**France's CNIL fines Google 150,000 euros for non-compliant privacy policy**

The CNIL, France's Data Protection Authority, issued a 150,000 € monetary penalty on Google Inc. on 3 January saying that Google's 2012 single privacy policy, applying to various Google services, does not comply with France's Data Protection Act. The CNIL ordered the company to publish a communiqué on this decision on its homepage Google.fr within eight days of its notification.

The CNIL's decision follows the EU Data Protection Working Party's assessment of the privacy policy which concluded that it failed to comply with the EU legal framework. In addition to France, Data Protection Authorities in the UK, Germany, Italy, the Netherlands and Spain started enforcement actions in 2013. Last December, Spain identified three serious violations of its data protection law and imposed a 300,000 € fine on Google for each one of them. The CNIL declared last summer that as Google processes data of users of Google services in France, it must comply with French law.

It requested Google to:

1. Define specified and explicit purposes;
2. Inform users with regard to the purposes of the processing implemented;
3. Define retention periods for the personal data processed;
4. Not proceed, without legal basis, with the potentially unlimited combination of users' data;
5. Fairly collect and process passive users’ data;
6. Inform users and then obtain their consent in particular before storing cookies in their terminal.

The CNIL now states, in connection with the monetary penalty:

*The company does not sufficiently inform its users of the conditions in which their personal data are processed, nor of the purposes of this processing. They may therefore neither understand the purposes for which their data are collected, which are not specific as the law requires, nor the*
ambit of the data collected through the different services concerned. Consequently, they are not able to exercise their rights, in particular their right of access, objection or deletion. The company does not comply with its obligation to obtain user consent prior to the storage of cookies on their terminals. It fails to define retention periods applicable to the data which it processes. Finally, it permits itself to combine all the data it collects about its users across all of its services without any legal basis.'

The 150,000 € penalty is the highest that the CNIL has issued to date. Google has not yet publicly commented on the monetary penalty.

Make-up and fake fingers – staying ahead of the online spoofers

Scammers can use masks and make-up to dupe face recognition software. Image courtesy of the EU-funded TABULA RASA project. Facial make-up and latex fingers engraved with someone else’s fingerprint used to be enough to fool identification software – but that’s about to change thanks to an EU project which is part of European efforts to beef-up authentication software and network security. Identification using facial features or fingerprints – known as biometric identification – was once seen as a way to a password-free future. However, they have proved all too easy to dupe – the fingerprint scanner on Apple’s iPhone 5S was hacked within days of its launch using just a photograph.

The EU-funded TABULA RASA project is coming up with ways to make biometric identification resistant to attack.

"The aim of the TABULA RASA project is to study the vulnerabilities of biometric systems in the context of spoofing attacks ... and in case of vulnerability, to develop counter measures to detect those kind of attacks,” said Dr Sébastien Marcel, the project coordinator. The three-year project set up the Spoofing Challenge where researchers developed new ways of attacking biometric systems. One successful attack involved the attacker using make-up to look more like the person she was trying to fake.

Researchers drew up a list of known spoofing attacks using experts, scientific papers and online sources, and those that were easiest to replicate were chosen for further research as these posed the most realistic threat. They recreated the attacks and recorded the data, which they then used to develop countermeasures to beef up biometric authentication systems such as face, fingerprint and voice identification software.

Flat face: They found, for example, that photographic spoofs on facial recognition systems can be identified by detecting how three-dimensional the face is. The flatter and more two-dimensional the face appears to be, the more likely it is to be a spoof.
The project also studied the effect of combining biometric identifiers to increase security. For example, a real finger can have moisture on it and blood running under its surface. Producing a fake finger to fool moisture and blood-flow sensors can be costly and time-consuming, making the spoofing attack more difficult and perhaps less likely to happen. “It can be hacked, but is it worth it?” said Dr Marcel.

He gave the hacking of the iPhone 5S’s fingerprint scanner as an example. While the method used to hack it was ‘nothing new’, it took days to do, by which point the owner could have locked their phone remotely. “You also have to steal the phone”, he added. Many of the countermeasures developed during the project are sold commercially by TABULA RASA’s industrial partners. This flow of information and innovation goes both ways, as the industrial partners on the project provide information on commercially available biometric systems and vital market insight for researchers.

Network security: Outside of biometric authentication, other EU-funded projects are developing new detection and protection techniques against computer viruses. The MALCODE project identifies a virus by the instructions it carries out on a computer. By detecting the virus at such a low level, the software bypasses many of the virus’ ways of fooling a system, such as encrypting its code.

In addition to researching attacks on individual computers, the EU funds projects investigating and improving the security of communication networks. Control systems for critical infrastructures, such as power grids, are rapidly moving from offline custom networks to more standardised online solutions.

“The aim of the TABULA RASA project is to study the vulnerabilities of biometric systems in the context of spoofing attacks.” Dr Sébastien Marcel, the coordinator of TABULA RASA

“Unfortunately this technological trend introduces new security issues, since in the new scenario critical infrastructures are increasingly exposed to cyber threats,” explained Prof. Salvatore D’Antonio, project manager for the INSPIRE project. Researchers on the project developed a system that prioritises important instructions for a critical infrastructure over other network traffic in the event of a fault or cyber attack. This means that network performance is not compromised for the critical infrastructure, even if the total capacity of the network is reduced by a fault or attack on part of it.

Similar to INSPIRE, the TClouds project developed a ‘cloud of clouds’ to make healthcare data and power-grid commands sent through the cloud more resilient to cyber attacks. Using the
system, a user can access multiple clouds containing identical information, so that if one cloud is compromised by a cyber attack or simply stops working, another cloud can take over. New EU projects, such as Privacy-Preserving Computation in the Cloud (PRACTICE), aim to create tools to make user data stored in the cloud unreadable by cloud providers, adding another layer of privacy to cloud computing.

The problems facing online security and biometric authentication research are similar, as Dr Marcel explained: “It's a bit like the virus-antivirus industry – the more attacks and countermeasures to those attacks you develop, the more you realize that you can find more attacks.”

Read more:
https://www.tabularasa-euproject.org/
http://www.tclouds-project.eu/

Snowden Testimony for European Parliament

On 7 March Edward Snowden gave answers on a series of questions posed by members of the LIBE committee of the European Parliament. As the responsible use of biometrics largely depends on protective measures by democratic legislators and Data Protection Authorities, it is important to highlight some of the answers Snowden gave regarding the way US, UK and EU intelligence agencies go below the legal radar by constructing secret data exchange mechanisms. In addition, the democratic legislative process, which is based on transparency and public debate, is severely being undermined by actions the NSA and GCHQ, that seeks to push European intelligence agencies either to push for national legislation to change in order to facilitate mass surveillance of unsuspected citizens, or to find holes in existing legislation. Snowden's testimony explicitly mentions these issues as follows:

“One of the foremost activities of the NSA’s FAD, or Foreign Affairs Division, is to pressure or incentivize EU member states to change their laws to enable mass surveillance. Lawyers from the NSA, as well as the UK’s GCHQ, work very hard to search for loopholes in laws and constitutional protections that they can use to justify indiscriminate, dragnet surveillance operations that were at best unwittingly authorized by lawmakers. These efforts to interpret new powers out of vague laws is an intentional strategy to avoid public opposition and lawmakers’ insistence that legal limits be respected, effects the GCHQ internally described in its own documents as ‘damaging public debate.’”

“The ultimate result of the NSA’s guidance is that the right of ordinary citizens to be free from unwarranted interference is degraded, and systems of intrusive mass surveillance are being constructed in secret within otherwise liberal states, often without the full awareness of the public.”

“By the time this general process has occurred, it is very difficult for the citizens of a country to protect the privacy of their communications, and it is very easy for the intelligence services of that country to make those communications available to the NSA.”
In addition Snowden further states, that in the UK Verizon, British Telecommunications, Vodafone, Global Crossing, Level 3, Viatel, and Interoute all cooperate with the GCHQ, to include cooperation beyond what is legally required.

When striving to the responsible use of biometrics this testimony needs some proper attention. If governments and private (ICT) companies can secretly pass public debate and scrutiny up to the legislative process, we may need to escalate to matter of responsible use of biometrics to our legislators and citizens by improving education provisions, awareness programs and public debate. Guidelines should be established regarding the actual content of a policy that ensures the responsible of biometrics, providing sufficient guidance for developing adequate requirements, specifications and legal provisions, up to the ingredients for dedicated legislation.

Read more: http://s3.documentcloud.org/documents/1061127/vjhvekoen1ww.pdf

UBIN launches USB biometric enterprise security device

UBIN has announced the launch of its new biometric enterprise security system, called MiKey. According to the Germany-based company, MiKey links a user's digital ID to their physical ID and does so by integrated a fingerprint reader, encryption, storage and Smart Card in a USB stick form-factor. UBIN also says the MiKey has an engineered ability to keep biometrics locked inside the device, complicating extraction.

NFC is set to be added later this year, to expand on MiKey, the company says.

"The MiKey solution is a great leap forward in information security and comes at a relevant time of increasing privacy concerns," Uwe Braun, UBIN’s Managing Director said. "By combining biometrics, encryption and storage in one highly integrated device, Enterprise customers are able to achieve an unprecedented degree of secure access to their data."

The MiKey will come in a variety of data storage capacities up to 32GB and will be available in the second quarter.

Read more: http://www.biometricupdate.com/201403/ubin-launches-usb-biometric-enterprise-security-device
3. Outside Europe

**International Standardisation now active for more than 10 years**

The international standardisation committee on Biometrics is now active for more than 10 years. ISO/IEC JTC1 SC37 has since generated numerous standards on application programming interfaces, data formats, profiles and best practices for applications, testing methodologies and jurisdictional issues. The full catalogue with completed standards as well as standards under development is available at:

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=333770&published=on&development=on

A very helpful standard both for the academic as well as for the industrial stakeholders is the standardized biometric vocabulary, which has been published as ISO/IEC 2382-37:2012. An online version of standardized terms and definitions contained in this standard is available at:

http://www.christoph-busch.de/standards.html

The work on further standards (e.g. biometric sample quality, XML encoding of data records) is ongoing. SC37 had its recent meeting in Darmstadt, Germany. The next working group meetings are scheduled for July this year to be held in Purdue, US.

**FICV: a new FVC-onGoing benchmark area on Face Compliance Verification to ISO/IEC 19794-5:2011**

FVC-onGoing (Dorizzi, et al., 2009) (BioLab, 2014) is a web-based automatic evaluation system, proposed to test biometric recognition algorithms on a set of sequestered datasets, and to report results using well-known performance indicators and metrics. The aim is to track the advances in recognition technologies, through continuously updated independent testing and reporting of performances on given benchmarks. The algorithms are evaluated using strongly supervised approaches, to maximize trustworthiness of the results.

FVC-onGoing is:
- an "on going competition" always open to new participants;
• an evolving online repository of evaluation metrics and results.

In the FVC-onGoing website a new benchmark area named Face Image ISO Compliance Verification (FICV): https://biolab.csr.unibo.it/fvcongoing/UI/Form/BenchmarkAreas/BenchmarkAreaFICV.aspx has been created to automatically perform the tests of the SDKs for the evaluation of face images to the ISO standard. In particular the framework is based on the indications provided by the ISO/IEC 19794-5:2011 standard (ISO/IEC 19794-5, 2011), designed starting from the guidelines initially proposed by ICAO. The standard specifies rules for encoding, recording and transmitting the facial image information and defines scene constraints, photographic properties and digital image attributes of facial images. The FICV benchmark area has been designed to automatically evaluate the SDKs able to automatically verify the compliance of face images to (ISO/IEC 19794-5, 2011), in the attempt of semi-automating the document issuing process.

Currently, this benchmark area contains the following benchmarks:
• **FICV-TEST:** A simple dataset useful to test algorithm compliancy with the testing protocol (results obtained on this benchmark are only visible in the participant private area and cannot be published).
• **FICV-1.0:** A large dataset of high-resolution face images related to all the requirements specified in Table I. This benchmark is described in detail in (Ferrara, Franco, Maio, & Maltoni, 2012).

Starting from the indications provided into the ISO standard, a set of 24 tests has been defined to evaluate the accuracy of automatic systems for compliance verification (Ferrara, Franco, Maio, & Maltoni, 2012). The tests can be organized into two categories:
• Feature extraction accuracy: this test evaluates the accuracy of eye centers detection;
• Photographic and pose-specific tests: the face must be clearly visible and recognizable;

This requirement implies several constraints that generate most of the uncertainties in the interpretation of the ISO standard. A precise formalization is here proposed to limit as much as possible the ambiguity.

An ad hoc database (containing 5588 images of 601 subjects; 310 fully compliant images and 5278 images not compliant to one or more characteristics) has been created combining public databases (i.e., AR (Martinez & Benavente, 1998), FRGC (Phillips et al., 2005) and PUT (Kasiński, Florek, & Schmidt, 2008)) and images internally acquired.

The database also contains the ground-truth data needed for an objective performance evaluation; in particular the following information is available for each image:
• coordinates of the eye corners;
• compliance to the requirements expressed on the basis of a three-state logic: i) compliant, ii) non-compliant and iii) dummy. The dummy value is used for the cases of uncertainty.
Performance evaluation is carried out on the basis of the two kinds of error that can be made by the software for compliance verification:

1. False Match (FMR): declaring compliant with respect to a given characteristic an image that is noncompliant;
2. False Non-Match (FNMR): declaring noncompliant an image that is compliant.

The FICV benchmark area, designed and realized within the FIDELITY European project, is now publicly available to the scientific community. The results of one SDK realized in FIDELITY have already been published on the FICV website.

References:

How to Apply International Human Rights Law to NSA Spying

Snowden revelations spark international debate on privacy and data protection. The Human Rights Committee commenced its one hundredth and tenth session in Geneva from March 10-28. During this session, the Committee will review the reports of several countries on how they are implementing the provisions of the International Covenant on Civil and Political Rights (ICCPR), an international human rights treaty and one of the bedrocks of human rights protections.

Countries that have ratified the ICCPR are required to protect and preserve basic human rights through various means including administrative, judicial, and legislative measures. Additionally, these countries are required to submit a report to the Human Rights Committee, a body of independent experts who monitor the implementation of States’ human rights obligations, every four years. The United States ratified the ICCPR in 1992 and is thus tied to these obligations, and required to regard the treaty the same as it would any domestic law. The Human Rights Committee will review the US’s human rights records on Thursday, March 13. In particular, the Committee will be scrutinizing the US’s mass surveillance practices and its compliance with Article 17 on the right to privacy.
At the opening session of the Human Rights Committee meeting, the UN High Commissioner for Human Rights, Navy Pillay, made it clear that the topic of privacy and surveillance is a priority:

"Powerful new technologies offer the promise of improved enjoyment of human rights, but they are vulnerable to mass electronic surveillance and interception. This threatens the right to privacy and freedom of expression and association."

Read more: https://www.eff.org/deeplinks/2014/03/how-un-human-rights-committee-should-apply-international-law-nsa-spying
Apple publishes whitepaper on iOS security, details Touch ID fingerprint sensor specs, functionality

February 28, 2014 - Apple has just launched a new whitepaper, explaining its security in iOS and goes into depth explaining how its fingerprint sensor in the iPhone 5S – the Touch ID – works. “[The Touch ID] reads fingerprints from any angle and learns more about a user’s fingerprint over time, with the sensor continuing to expand the fingerprint map as additional overlapping nodes are identified with each use,” the whitepaper explains.

According to the whitepaper, the sensor can be trained to recognize up to five different fingers, but fingerprint data is not available to other apps or third parties. “With one finger enrolled, the chance of a random match with someone else is 1 in 50,000. However, Touch ID allows only five unsuccessful fingerprint match attempts before the user is required to enter a passcode to obtain access.” As for fingerprint recognition, the company says the sensor is only active when the capacitive steel ring that surrounds the Home button detects the touch of a finger.

Reported previously in BiometricUpdate.com, in November 2013, the USPTO published a patent filed by Apple for its Touch ID sensor. According to the company, “the 88-by-88-pixel, 500-ppi raster scan is temporarily stored in encrypted member within the Secure Enclave while being vectorized for analysis, and then it’s discarded after. The analysis utilizes subdermal ridge flow angle mapping, which is a lossy process that discards minutia data that would be required to reconstruct the user’s actual fingerprint. The resulting map of nodes never leaves iPhone 5S, is stored without any identity information in an encrypted format that can only be read by the Secure Enclave, and is never sent to Apple of backed up to iCloud or iTunes.” Decrypted class keys are held in memory and are lost if the device is rebooted. In addition, says the company, the Secure Enclave will discard keys after 48 hours or 5 failed Touch ID recognition attempts.

Apple was an early player with an embedded fingerprint sensor, but the space is heating up with new competition. Earlier this spring, Samsung launched its Galaxy S5 with an embedded fingerprint sensor.


Frost and Sullivan – Biometrics in cell phones

February 25, 2014 - Biometrics in cellphones is a major trend, and Frost & Sullivan has just published a new report looking at exactly that, called Biometrics in Cellphones.
Samsung just launched its Galaxy S5 with a fingerprint sensor, Apple launched the iPhone 5S in September last year and there is a whole slew of phone manufacturers in Asia and elsewhere around the world that have already integrated fingerprint technology into consumer devices. Facial recognition has been an option in the Android operating system for quite some time, voice recognition is making an appearance in a growing number of handsets, iris recognition is an emerging capability for mobiles and most recently, fingerprint sensors are being embedded in hardware.

According to Frost.com, the study focuses on growth in the biometrics devices market worldwide with special attention on India as having a mass demand for online transactions facilitated by biometrics, and also a huge availability of feature phones supporting secure authentication.

Frost & Sullivan certainly isn’t the only firm to take a close look at this trend. The Biometrics Research Group has long-predicted that smartphones would soon include biometrics. According to the group, “U.S. consumers will use smartphones and tablets to make retail purchases of approximately US$35 billion in 2013, compared with US$20 billion in 2012.”


IDEX and CrucialTec partner up for mobile touch sensors

February 25, 2014 - IDEX ASA has announced that its previously undisclosed mobile communications partner is in fact, CrucialTec.

According to IDEX, the combined strength of the two companies offers major smartphone and mobile device manufacturers IDEX sensors along with CrucialTec’s mass manufacturing, industrial knowhow and supply capabilities. CrucialTec is a manufacturer of the “biometric track pad,” which is exactly what it sounds like: a track pad that reads fingerprints.

The two companies are currently working to design a small-area mobile touch sensor sampling for the first quarter of this year, 2014. Also, IDEX is concurrently continuing the development of its polymer-based flex sensor technology, which combines IDEX and PicoField technology. Reported previously, IDEX acquired PicoField last year.

“We are extremely pleased to disclose our partnership with CrucialTec and excited with our near-term plans to commercialize high-performance touch sensor solutions to address significantly increased customer interest and rapid market adoption of fingerprint sensors,” Hemant Mardia, CEO of IDEX said. “This collaboration brings forward the first touch fingerprint sensor solution into the mobile market from IDEX, addressing strong market pull. The combination of IDEX’s advanced, best in class, patented sensor technology and CrucialTec’s patent-protected packaging technology, proven high-volume production capability and tremendous reach and relationships with major OEMs represents a powerful value proposition for the mobile market.”

Read more: www.idex.no
Cognitec Algorithm Receives Best Rating in NIST Independent Vendor Test

Dresden, April 7, 2014—Test results on the performance of automated age estimation algorithms, published by the National Institute of Standards and Technology (NIST), confirmed Cognitec Systems’ market-leading position in the face recognition market. The test compared nine algorithms submitted by six participants, five companies and one university, and applied them to seven million images. Results show that Cognitec’s algorithm performs with the highest accuracy for all age groups. Most notably, the algorithm shows superior performance “in the youth and senior age groups, leading the next most accurate algorithm in 5-year accuracy by 30% and 16%, respectively,” according to the report.

Complete NIST report: www.nist.gov/customcf/get_pdf.cfm?pub_id=915238

The Swiss Center for Biometrics Research and Testing is born!

A brand new Swiss Center for Biometrics Research and Testing, third one of its kind in the world, has been officially launched this Tuesday, April 8th in Martigny, at the heart of the Idiap Research Institute, a key actor of biometrics on the international scene. The creation was saluted during a press conference in the morning of April 8 by the management of the institute, but also by the cantonal authorities and the City of Martigny.

Read more: www.biometrics-center.ch/news/a-european-first-in-martigny
5. Events

EAB seminar on biometrics for financial transactions, Berlin May 21: special rates for EAB members

The one day workshop will reflect the opportunities of biometrics in the financial market, with a focus on successful implementations and use cases. We will discuss, how processes can be designed both biometrically protected and privacy compliant. The speakers are all members of the European Association for Biometrics (EAB) and intend to provide you with their experience how to take best benefit of biometric techniques in the area of banking and other financial transactions.

The seminar will be moderated by Christoph Busch from Fraunhofer IGD, also Professor at the Gjøvik University Norway and member of the EAB Board.

Read more: http://www.eab.org/events/program/66


SDW2014 will provide a global showcase for next generation human identity solutions, focusing on intrinsic document security and on the new cutting edge secure infrastructure now required to produce and use these advanced documents in live situations. There will be a special focus on biometrics, document fraud detection and intelligent border control. The event takes place at the Queen Elizabeth II Conference Center. You can book your ticket for a reduced price by marking the 'Association Member Rate' at the delegate booking page of the SDW2014 website (www.sdw2014.com).

Read more: www.sdw2014.com/delegate-booking/

European Biometrics Research and Industry Awards 2014: call for candidates

The European Association for Biometrics (EAB) is launching the eighth European Biometrics Research and Industry Awards. These prestigious awards are granted annually to individuals who have been judged by a panel of internationally respected experts to be making a significant contribution to the field of biometrics research and innovation in Europe.

The award is stimulating innovation in academic research as well as in industry. Thus biometric experts with either of the following profiles should submit their work. Academic researchers enrolled in the last or penultimate year of a Ph.D. program or who have obtained a Ph.D., with major focus on biometrics, from a European academic institution no later than two years before the given deadline, might consider applying for the awards. Further industrial researchers employed by European companies whose core business is biometrics
might consider applying for the industry award, which will be granted to the candidate that has created the strongest impact for industry.

Applicants are asked to submit a research paper and supporting information by 15 May, 2014. These papers will be reviewed by a jury composed of internationally recognized experts in the field of biometrics who will judge the academic and scientific quality for the EAB academic research award and the novelty, impact, applicability and other business aspects for the EAB industry award.

For all information about the award including Application Forms, Templates, and the Rules, please visit: http://www.eab.org/award/cfp.html.

You can also contact the chair of the award committee, Prof. Patrizio Campisi: patrizio.campisi@uniroma3.it

EAB Research Projects Conference (EAB-RPC) 2014, Darmstadt 8-9 September 2014

Biometrics and Identity Management are key research topics that are currently investigated in a number EU-projects running under the seventh Framework program. International research is dealing with innovative solutions for secure and privacy compliant biometrics and federated identity management.

The EAB and the EU-projects FIDELITY, FastPass, BEAT, Future-ID, INGRESS, are jointly organizing a Research Project Conference (EAB-RPC), to present research results and in order to discuss the benefit of this research for our European society. Moreover experts from the biometric community will discuss on a panel Ethical and Privacy Issues of Biometrics and Identity Management. Furthermore a second panel will be devoted to discuss and identify future research topics in the Horizon2020 research program.

Read more: http://www.eab.org/events/program/69

International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt 10-12 September 2014 – Call for Papers

The BIOSIG 2014 is Europe’s state of the art conference on Biometrics that will present innovations and best practices in key areas of biometrics R&D that can be transferred into future applications. The 13th edition of this international conference addresses various topics, such as biometric standards and interoperability, multimodal and multi-biometrics (sensor, modality, sample, feature, score and decision fusion), security analysis of biometric components or systems, on-card comparison, fake resistance, liveness detection, aging of reference data, template protection, derivation of cryptographic keys from biometrics, biometric middleware, user interface design for biometric systems, biometric performance measurement, sample quality, best practices, usability, forensics and other emerging applications, ethical, legal and socio-technological aspects, biometrics for public administrations.
The conference is jointly organized by the following organizations:

- Competence Center for Applied Security Technology (CAST)
- German Federal Office for Information Security (BSI)
- European Association for Biometrics (EAB)
- Joint Research Centre of the European Commission (JRC)
- TeleTrusT Association
- Norwegian Biometrics Laboratory (NBL)
- Center for Advanced Security Research Darmstadt (CASED)
- Fraunhofer Institute for Computer Graphics Research IGD
- Special Interest Group BIOSIG of the Gesellschaft für Informatik e.V. (GI).

Interested EAB members that want to contribute a presentation to BIOSIG 214 should submit a paper prior to May 15, 2014. The final program of the conference will be published in July 2014.  

Read more: http://www.biosig.de/biosig2014

ID World International Congress - Call for Papers, 18-20 November 2014

The ID World International Congress is the prime conference on the evolving world of identification. It is the only international forum that looks at the advanced ID industry as a whole, rather than focusing on a specific technology or vertical sector. Delegates from all over the world will meet in Frankfurt am Main, Germany, from 18-20 November 2014 to learn from their peers and network among experts in the conference as well as in the Euro ID exhibition.

Please send in your abstract about biometrics, RFID, smart card technologies and data collection by 7 May 2014.  

Read more: http://www.mesago.de/de/EID/home.htm

International Joint Conference on Biometrics - IJCB’14, Clearwater Beach, USA 29 September – 2 October

International Joint Conference on Biometrics (IJCB 2014) combines two major biometrics research annual conferences, the Biometrics Theory, Applications and Systems (BTAS) conference and the International Conference on Biometrics (ICB). The blending of these two conferences in 2014 is through special agreement between the IEEE Biometrics Council and the IAPR TC-4, and presents an exciting event for the entire worldwide biometrics research community. The success of IJCB 2011 organized in Washington DC during September 2011 has generated huge support from the biometrics community to repeat such blending of two conferences in the year 2014. This conference is a result of major worldwide consensus to join the two major biometrics meetings and to establish IJCB as a venue for presenting biometrics research results of highest quality.

Read more: http://ijcb2014.org/
6. Reports

European Standardisation in CEN

The CEN TC224 Working Group 18 “Interoperability of biometric recorded data” met at the Fraunhofer IGD in Darmstadt at March 13/14, 2014. Experts from Austria, France, Germany, Italy, Norway, Spain, UK, and ANEC took part in this meeting and discussed the following topics:

- Project on “Biometric application profiles for law enforcement and border control authorities using portable identification systems”
- Project on “Environmental influence testing methodology for operational deployments of European ABC systems”
- Transition of CEN/TS 16428 “Best Practices for slap ten-print captures” to ISO/IEC JTC 1/SC 37 as basis for an ISO project
- CEN/TS 16634 “Recommendations for using biometrics in European Automated Border Control” is about being published
- Registration of the project “Detection of suspicious biometric samples for European Automated Border Control” in the TC224 program of work
- An initiative to publish ISO/IEC 2382-37 “Biometrics Vocabulary” with (initially) German and French translations in an European Standard. Volunteers for other European languages are appreciated.
- Possible actions of WG 18 on Privacy-by-Design in biometrics

The next WG 18 meetings will take place May 15/16 in Paris and October 8/9 in Madrid. Interested experts willing to contribute to the Projects of WG18 are strongly encouraged to contact the group via their National Standards Body.

1st International Symposium on 3D Face Recognition Twente

On 10 October 2013, a one day symposium on 3D Face Recognition was organised at the University of Twente, The Netherlands. The event was sponsored by the IEEE Benelux Chapter on Signal Processing and supported by the European Association for Biometrics. Nine invited speakers presented work on 3D Face projects in general and in more detail on specific research like 3D reconstruction from image sequences, 3D shape matching, 3D landmarking, 3D Ear Recognition and 3D Face Recognition in Industry and Forensics. The speakers from 4 different countries in Europe, from The University of Twente, K.U. Leuven, Morpho, CASED and the NFI ensured a very interesting and successful symposium. In total more that 80 participants were present at the symposium. The participants were from different countries, from research institutes (both researchers and students), industry, police and forensics. Organiser and chair of the day was Luuk Spreeuwers of the new Chair for
Biometric Pattern Recognition of the Services, Cyber Security and Safety Group at the University of Twente.

Slides of the workshop are available at: http://eab.org/events/program/44

NBL Annual Workshop 2014

Instead of using passwords, voice recognition or your typing on your keyboard may become the new way of authenticating yourself. On 28th of February the Norwegian Biometrics Laboratory at Gjøvik University College arranged a workshop focusing on continuous authentication and behavioral biometrics.

What are the challenges and possibilities of behavioral biometrics compared to biological biometrics or other authentication methods, and how can we secure computers better by continuously checking the identity of a user?

On February 28th 2014, The Norwegian Biometrics Laboratory in Gjøvik gathered speakers from academics and industry to focus on these subjects. Continuous authentication of users can as an example be measured of how the user types on the keyboard, how the user uses the mouse, whether the user is using ctrl + p or the print icon to print something, or how he changes between various applications. In some years we might use voice recognition to log onto our personal computer.

Bjørn Erik Thon from The Norwegian Data Protection Authority gave an introduction of how the authorities are working and thinking about protection of privacy and technology developments. Mark Nixon from the University of Southampton was the keynote speaker of the workshop. He reported about his research within gait recognition and soft biometrics for surveillance. In soft biometrics certain features of a person are determined, like gender, ethnicity, body shape, and hair length and color. Each of these features are not enough to identify a person, but will help in the total identification process.

Slides of the workshop are available at: http://eab.org/events/program/40
German Biometrics Working Group Meeting

The EAB partner organization TeleTrusT (TTT) is a large-scale network of IT-Security related institutions that is operating the German Biometrics Working Group. This group of biometric experts assembled on March 25th for its spring meeting in Darmstadt and featured numerous reports on biometric applications and most recent research results.

Highlight of the day was the presentation of Matthias Grell (German Border Police), who reported about the deployment of the Automatic Border Control Gates EasyPASS, which is currently focused on the international airports Frankfurt, Hamburg and Munich. The system is designed for a False Reject Rate below 2% and is targeted to cope with an increasing passenger flow since one border control officer can be in charge for video based supervision of six control gates. Also an operational report from a financial application was presented by Malte Kahrs from the most recent EAB-member MTRIX that has introduced two factor authentication based on password and fingerprint recognition for more than 19,000 subjects working for German Saving Banks. Remarkable is the extremely low failure-to-enrol rate which constitutes only 3 incidents. A research report for EMV-compliant payment smartcards with biometric On-Card-Comparison was provided by Olaf Henniger (Fraunhofer IGD). Again Data Privacy and Biometric Template Protection was in focus of this event: Christian Rathgeb (Hochschule Darmstadt) presented latest research on Bloom-filter based iris template protection that has proven to provide security (i.e. protection of reference data) and a significant speed-up for identification systems without loss of biometric accuracy compared to a plain-text biometric system.

Slides of the meeting are available at: [http://eab.org/events/program/54](http://eab.org/events/program/54)

NIST International Biometric Performance Conference – IBPC-2014

On April 1-3, 2014 more than 100 participants from 12 nations followed the invitation by the U.S. NIST in Gaithersburg to attend the 3rd International Biometric Performance Conference that took place in Gaithersburg, U.S. The conference focused on performance and testing methodologies of biometric components and systems and provided a valuable platform to discuss how biometric technologies are being tested, certified, and upgraded.

The presentation of the NFIQ2.0 prototype and other biometric sample quality measures was one of the highlights indicating how empirical studies and innovative algorithm can contribute to higher system performance. NFIQ2.0 will be released as open source later this year. Further security aspects such as Presentation Attack Detection (i.e. spoof detection) capture devices as well as biometric template protection for verification and identification applications were discussed. The latter is specifically of interest in the context of ISO/IEC 30136, which is developing a testing protocol incorporating security testing of protection...
schemes. Moreover, ePassport use cases and operational testing of Automated Border Control with rapidly growing application in numerous countries were covered. Very impressive was the report about the Indian Aadhaar system that has to date enrolled more than 620 million citizens, which impacts multiple trillions de-duplication comparisons per day at an enrolment rate of 1 million residents per day. Furthermore, usability testing of biometric capture devices was discussed for which the validation of the ISO/IEC 24779 icons and symbols for guiding capture subjects was the most relevant aspect. The talks covered operationally relevant themes and gave insight into the design, procurement, and what operators require from test and evaluation activities. Last but not least, forensic testing was covered with an outreach on human examiners white-box testing. Overall the conference and the embedded EAB-organized session on template ageing not only presented novel evaluation methodologies and recent trends in testing but also indicated future research needs. The next IBPC will take place in spring 2016.

The presentations from IBPC-2014 will be available at: http://www.nist.gov/itl/iad/ig/ibpc2014.cfm

**NIST EAB Session on Biometric Ageing at the IBPC-2014**

On the 3rd of April 2014 the European Association of Biometrics organized a special session on "Age Factors in Biometrics" in conjunction with the International Biometric Performance Testing Conference 2014 which was chaired by EAB member Christian Rathgeb.

The session included a total number of seven talks, which covered potential ageing effects with respect to different biometric characteristics in particular fingerprints, iris, face and voice, as well as other issues.

Christian Rathgeb opened the session by giving perspectives to the issuance of breeder documents in particular, birth certificates, in the European Union, which include potentially include biometric information. Günther Schumacher from the EU-Joint Research Center and Soweon Yoon from the Michigan State University discussed biometric performance of fingerprint recognition systems over long time spans. Yunlian Sun from the University of Sassari presented a short-term and long-term aging analysis in human faces.

Patrick Grother from NIST presented a study on ageing effects on iris biometrics based on operational
data obtained from crossings at the Canadian/US border. This study which relates to the NIST IREX VI Report was heavily discussed with Kevin Bowyer from the University of Notre Dame, who himself is an expert on the topic of iris biometric ageing. Finally, Norman Pooh gave an insight on the effects of biometric ageing on multi-biometric recognition systems based on face and voice.

The session was well attended by the participants of IBPC’14 and provided many interesting perspectives to this rather young area of biometric research.

The presentations from IBPC-2014 will be available at: http://www.nist.gov/itl/iad/ig/ibpc2014.cfm

EAB Workshop on Forensics and Biometrics 2014

On 17 January 2014 a workshop took place in Darmstadt (Germany) on biometrics and forensics in Europe, organized by the Biometrics and Forensics Working Group of the European Association for Biometrics. The workshop was a first step in a series of activities planned by the working group chair, Didier Meuwly (The Netherlands Forensics Institute).

Report of the Workshop

After a short opening and introduction about the EAB by Max Snijder (Secretary of the Board), Didier Meuwly proceeded with going through the topics of the workshop, including the objectives of the Forensics and Biometrics Working Group.

Geoff Withaker kicked off with an overview of forensics biometrics landscape in the UK. The variety of parameters call for standardization (exchange formats, language ....). He elaborated on the key stakeholders and governance. This requires a lot of coordination with a lot of different people and organizations. To finalize John talked about the quality of facial images for policing purposes, while pointing to the differences between using images for civil and policing purposes. 3D facial images may well fit into a forensic biometrics environment. There is an increasing movement towards mobile, the crime scene is being digitized. Also digital crimes don’t leave physical traces such as fingerprints or DNA. More to see ‘lights out systems’, ruling out fingerprint experts/adjudicators.

Peter Hanel then presented on interoperability issues with the Prüm-treaty (and associated systems) as an example. The EU has different bodies to take decisions. Member States were not happy with the speed, so they decided to agree on a bilateral treaty, now the Prüm Treaty. The EC took the Prüm Treaty as EU standard and turned it into EU legislation. Prüm-treaty involves fp-data (+ palm print), DNA profiles and Vehicle registration data. Prüm has no central system. Prüm partners opt for an automated requesting procedure (lights-out). Trend: using technology that already exists. A bilateral system is complicated, but it works.

Ambika Suman (CAST UK Home Office) was speaking on the topic of 'Examiner Assisted Biometrics Systems' (i.e. reliant on the input and interaction of a human interaction). With
this kind of systems only the actual matching is automated. Clearly EABS's work off line and are rather a balancing of expertise and capabilities, than replacement of one for the other. The requirement for having an examiner intervention may be politically motivated. Further Ambika elaborated on the differences between Conventional non-Police Design Requirements and Police Design Requirements. Poor quality of images is still an issue. It was questioned whether an examiner could help to better exploit 3D/multiple views imagery or matching techniques for poor images. There is no clear understanding how humans perform recognition. More knowledge about this could be useful for algorithm development.

Jim Wayman continued the session with his presentation on speaker recognition and its legal acceptance in court cases. For that he used a real case that appeared summer 2013 in the US. From WOII speaker recognition evolved from the Analogue Sound Spectograph to Digital Speaker Recognition in current days. Controversy existed about the validity and reliability of the spectrographic approach for speaker recognition. A second approach on SR is based on phonetic/phonemic. This is without the aid of computers, so it can't be scaled. The 3rd approach focuses on speaker recognition. The scientific topic of a comparison of two voice specimens remains difficult. For example: voice stress is still difficult to accommodate. It is not know how to accommodate voice stress. Standardization on voiceprint format is ongoing. Clearly for voice recognition we need standards for examination, laboratory and accreditation standards, and standards for the collection and transmission of the data.

The speaker recognition (SR) topic was followed up by Stefan Gfroerer, who zoomed into current practices and future directions in R&D. Limited quality and quantity of audio material is a general problem in voice forensics. Various influences can have negative consequences on the usability and reliability of SR (circumstances, behavioral etc.). COTS are being used, but they are black boxes. Therefore governments build their own systems. COTS voice recognition products are incompatible and have problems with low quality, short voiceprint and voice disguise. Speaker recognition methods by machines vary widely, not for the better. Currently we don't see many activities to improve this situation, probably due to limited demand.

The final presentation is about research topics in forensic face recognition by Raymond Veldhuis. In forensic investigation typically low quality surveillance images are being compared with controlled quality images stored in a database. A more challenging task is forensic intelligence. Here images from one crime scene are being compared with images from another crime scene, which means low quality at both sides. Raymond elaborated on
the main challenges on creating and interpreting matching results. COTS black boxes are not a problem as such, as long as they can be calibrated. Calibration is being done based on representative reference data.

Panel Discussion: During the panel discussion the discussion came about the current lack of the ISO standards regarding forensic biometric data. The difficult question of the assessment of the quality of the forensic biometric data also emerged. As an answer the participants to the panel discussion explained that the questions related to forensic biometric data are multiple and therefore the notion of quality is multiple as well, and cannot be solved by a simple algorithmic approach.

The forensic sample reference may contain more than one form of information (a sound sample may include voice, background noise, and other sounds/noises). This requires a more complicated/sophisticated definition of quality. However, it may be difficult to put a single quality metric on a voice/sound print/recording. This will be difficult to make more objective, because there may be multiple purposes e.g. to a single voice/sound sample.

In order to harmonize the method of measuring of data quality in a forensic way it is needed that reference databases and samples of an exchangeable quality level are created. This could be done for all electronic imagery and data that are coming in. However, a the first step needs to be that the procedures for collecting are harmonized. It was also mentioned that there should be a technical standard defining the metrics/threshold so it can be decided whether or not a sample can be used in court.

Conclusions: It was decided that a white paper will be written summarizing the inputs and contributions of this workshop with the speakers and to use the result as a roadmap for the establishment of the permanent Forensic Biometric Committee of the EAB. The topics and issues that came out of the panel discussion will be input for further elaboration by the working group.

The presentations of the workshop on forensic biometrics the European Association for Biometrics and the NFI organized during the ISO/IEC JTC 1 SC 37 conference are available for EAB members through the EAB website: www.eab.org/events/program/55
Publisher: European Association for Biometrics
Editors: Christian Rathgeb, Max Snijder
Production: European Association for Biometrics
Contact: m.snijder@eubiometricsgroup.eu / secretariat@eab.org
Phone: +31 624 603809
Web: www.eab.org