EAB Newsletter January 8, 2018

EAB Newsletter revised: new format for more convenience

The format of the EAB newsletter has been revised. It is now brought into html-format and only contains a brief introduction to the article. When you click on 'Full Story' you will be redirected to the members section of our website for the full article by using your login credentials.

Full story

Security Union: Commission closes information gaps to better protect EU citizens

Today, the European Commission has proposed to close information gaps by upgrading EU information systems for security, border and migration management and making them work together in a smarter and more efficient way. The measures will enable information exchange and

Full story

EU DPAs: Legal action to come unless Privacy Shield improved by 25 May 2018

The EU Data Protection Authorities say that they have, despite improvements to the Privacy Shield framework, identified a number of significant concerns that need to be addressed both by the EU Commission and the US authorities. The DPAs, together as the Article 29

Full story

Table of contents

Next events:

September 24 - 25, 2018: EAB Research Projects Conference (EAB-RPC) 2018

September 25, 2018: 8th EAB General Assembly

September 26, 2018: German TeleTrusT Biometrics Working Group

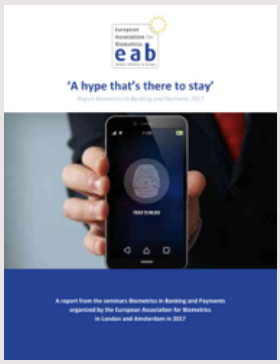
September 26, 2018: EAB Biometrics Research and Industry Awards 2018

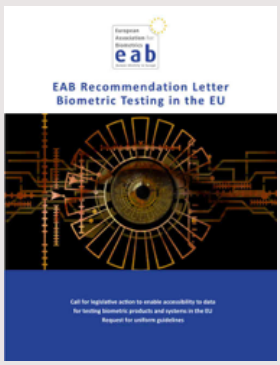
September 27 - 28, 2018: BIOSIG 2018 - 17th International Conference of the Biometrics Special Interest Group

November 9, 2018: Seminar on Biometric Data and the GDPR

November 23, 2018: Norsk Biometri Forum Meeting

Special reports:





EAB Biometric News, January 8, 2018

EAB Newsletter revised: new format for more convenience

18 December, 2017

The format of the EAB newsletter has been revised. It is now brought into html-format and only contains a brief introduction to the article. When you click on 'Full Story' you will be redirected to the members section of our website for the full article by using your login credentials.

The old newsletter was quite large (sometimes more than 30 pages) and was sent in PDF as an email attachment. Now the EAB Newsletter will be smaller and more easy to access. It will be sent out more frequently (approx. every 2 - 3 weeks). The newsletter will be displayed into your email browser, including Outlook. The events calender will be included, showing the upcoming EAB activities. A special section presents reports from EAB events or other documents that are in the interest of our community.

All EAB members are invited to submit content for the newsletter. This can be about achievements in research and development, new projects in the area of biometrics and idientity in Europe and abroad, developments in EU policy making, projects on national ID, health care or financial services etc. For each newsletter the editors Christain Rathgeb and Max Snijder will compose a new set of articles and other content. For any suggestions you can contact Max Snijder at secretariat@eab.org.

EAB Biometric News, January 8, 2018

Security Union: Commission closes information gaps to better protect EU citizens

Strassbourg, 13 December 2017

Today, the European Commission has proposed to close information gaps by upgrading EU information systems for security, border and migration management and making them work together in a smarter and more efficient way. The measures will enable information exchange and data sharing between the different systems.

The measures will enable information exchange and data sharing between the different systems and ensure that border guards and police officers have access to the right information exactly when and where they need it to perform their duties, whilst ensuring the highest data protection standards and full respect of fundamental rights. In the context of recent security and migratory challenges, the proposal will ensure greater safety of EU citizens by facilitating the management of the EU's external borders and increasing internal security.

First Vice-President Frans **Timmermans** said: *"Speed counts when it comes to protecting our citizens against terrorism and saving lives. At this moment our EU information systems for security and border management are working separately which slows down law enforcement. With our proposal they will become fully interoperable. That means that law enforcement anywhere in the EU will be able to work directly and instantly with all the available information."*

Commissioner for Migration, Citizenship and Home Affairs Dimitris **Avramopoulos** said: *"Today we are delivering the final and most important element of our work to close gaps and remove blind spots in our information systems for security, borders and migration. From now onwards, border guards, immigration and police officers should have the right information at the right time to do their job. This is a flagship initiative for this Commission, and I urge the co-legislators to also make it their priority and complete their work within 2018."*

Commissioner for the Security Union Julian **King** said: *"Terrorists and serious criminals should not be able to slip through the net or under the radar. This is an ambitious new approach to managing and using existing information: more intelligent and targeted; clamping down on multiple identities and reinforcing effective police checks; connecting the dots to protect EU citizens while also protecting data by design and by default."*

Currently, EU information systems do not talk to each other – information is stored separately in unconnected systems, making them fragmented, complex and difficult to operate. This risks pieces of information slipping through the net and terrorists and criminals escaping detection by using multiple or fraudulent identities, endangering the EU's internal security and making border and migration management more challenging. The measures proposed today will plug those gaps and make sure that information provided to border guards and police is complete, accurate and reliable. The new tools will help better detect people who pose a threat not only when crossing EU borders, but also when travelling within Schengen. By simultaneously cross-checking information in different databases and streamlining access by law enforcement, the new tools will quickly alert border guards or police if a person is using multiple or fraudulent identities. It will also help to better identify vulnerable people such as unaccompanied minors, while making sure that fundamental rights and data protection are fully respected.

Connecting the dots and removing blind spots

Today's proposal introduces new elements to make a more intelligent and targeted use of the information available in the existing and future systems. This will allow national authorities:

- **to make best use of existing data. A European search portal** will provide a "one-stop shop" on a computer screen when border guards or police officers are verifying identify documents. Rather than having to decide which database to check in a particular situation, officers will be able to simultaneously search multiple EU information systems. This will put an end to information gaps and ensure that officers have a complete picture of a person without delay.
- **to detect multiple identities and counter identity fraud. A shared biometric matching service** will use biometric data, such as fingerprints or facial images, to scan existing databases and enable detection of information in different EU information systems. A **common identity repository** will provide basic biographical and biometric information, such as names and dates of birth of non-EU citizens, so that they can be reliably identified. Building on these, a multiple-identity detector will immediately flag to border guards and police cases of fraudulent or multiple identities.
- **to carry out rapid and effective checks.** When carrying out checks within a country, police officers will be able to query the identity data of third-country nationals and confirm who they are, including for the purpose of detecting multiple identities.

The Commission is also proposing a two-step approach for those law enforcement officers preventing, investigating, detecting or prosecuting serious crime or terrorism to **access the information** they need on third-country nationals in non-law enforcement systems. In full respect of data protection, the approach clarifies that as a first step searches will be carried out on a "hit/no hit" basis. As a second step, if a "hit" is generated, law enforcement officers can request access to the information needed in line with the respective rules and safeguards. To ensure that border guards and police officers have complete and accurate information at hand, data **quality control mechanisms** will also be created.

Building resilience on all fronts

Today, the Commission has also reported on the progress made on other security related priority files including the ongoing legislative proposals to strengthen information systems and the correct implementation and full application of existing legislation and instruments. The **12th Security Union report** takes stock of actions taken to deny terrorists the means to act, strengthen cyber resilience, counter radicalisation online and offline, and build up the external security dimension.

Link: http://europa.eu/rapid/press-release_IP-17-5202_en.htm

Background

President Juncker's State of the Union address in September 2016 highlighted the importance of overcoming the current shortcomings in data management and of improving the interoperability of existing information systems. Recent terrorist attacks have brought this into even greater focus, highlighting the urgent need for information systems to be interoperable, and to eliminate the current blind spots where terrorist suspects can be recorded in different, unconnected databases under different aliases.

In April 2016, the European Commission presented a Communication on stronger and smarter information systems initiating a discussion on how to make EU information systems work better to enhance border management and internal security. As part of an inclusive and transparent process the Commission set up a high-level expert group on information systems and interoperability to take this work forward and to address the legal, technical and operational challenges to achieve interoperability. The high-level expert group presented its final report in May 2017 setting out a range of recommendations. Building on those recommendations, the Commission proposed a new approach to achieve interoperability of EU information systems for security, border and migration management by 2020 and announced its intention to present, as soon as possible, a legislative proposal on interoperability. This was followed by a joint discussion between the European Parliament, the Council and the Commission on the way forward on interoperability.

In June 2017, the European Council reiterated the need to act and invited the Commission to prepare, as soon as possible, draft legislation enacting the recommendations made by the high-level expert group. In the context of 2018 Work Programme, the Commission announced that a proposal on the interoperability of information systems will be presented by the end of 2017.

EAB Biometric News, January 8, 2018

EU DPAs: Legal action to come unless Privacy Shield improved by 25 May 2018

Privacy, Law & Business, December 06, 2017

The EU Data Protection Authorities say that they have, despite improvements to the Privacy Shield framework, identified a number of significant concerns that need to be addressed both by the EU Commission and the US authorities. The DPAs, together as the Article 29 DP Working Party, demand an action plan to be set up immediately to address the appointment of an independent US Ombudsperson (currently there is an acting Ombudsperson).

The DPAs also call for rapid appointment of new members to the vacancies on the Privacy and Civil Liberties Oversight Board (PCLOB). Unless their concerns are resolved by 25 May 2018 when the EU GDPR enters into force, the DPAs will bring the Privacy Shield Adequacy decision to national courts for them to make a reference to the Court of Justice of the European Union for a preliminary ruling.

The DPAs have in their review focused on the assessment of both the commercial aspects of the Privacy Shield and on the legal framework relating to government access to personal data transferred from the EU for the purposes of Law Enforcement and National Security, including the legal remedies available to EU citizens.

Their review is separate from the recent review by the EU Commission, which was more positive but also pointed out the questions of the Ombudsperson and the missing members of the PCLOB, see

https://www.privacylaws.com/Publications/enews/International-E-news/Dates/2017/10/EU-Commission-EU-US-Privacy-Shield-works-but-implementation-can-be-improved/

The WP29 acknowledges the progress with Privacy Shield in comparison with the invalidated Safe Harbor, and offers to advise US authorities in drafting new guidance, in particular regarding HR data and onward transfers.

The DPAs' report on the Privacy Shield was adopted at their November Art 29 WP Plenary, which also adopted guidelines on consent and transparency as well as its updated referentials on adequacy and BCRs for controllers and processors. These documents will be published on the WP29 website in the coming days and are open to public consultation for 6 weeks before their final adoption.

The DPAs have also worked on tools for cooperation between DPAs on data breach notifications. It is expected that they will, in their February meeting, adopt guidelines on certification.

The DPAs' Privacy Shield report is at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 (see under Plenary meetings).

Read more about these developments in Privacy Laws & Business International Report. To subscribe, go to www.privacylaws.com/publications

EAB Biometric News, January 8, 2018

15th International Summer School for Advanced Studies on Biometrics for Secure Authentication

Alghero, Italy, 22 December 2017

The 2018 International Summer School on Biometrics will take place in Alghero, Italy, at June 11 -15. For fifteen years, the Summer School has been closely following the developments in science and technology to offer a cutting edge, intensive training course, always up to date with the current state-of-the-art. The school is open to about 50 highly qualified, motivated and pre-selected participants. To participate it is needed to send a filled application form together with a short curriculum vitae. Advance pre-registration closes by 15 February 2018.

The 2018 Summer School will zoom into the most up-to-date core biometric technologies developed in the field. The potential impact of biometrics in forensic investigation and crime prevention will be discussed, as well as how to detect impersonation attacks and disguise.

In this 15th edition, the courses will mainly focus on new and emerging issues:

- **How Biometrics can deal with impersonation and disguise;**
- **How to exploit new biometric technologies in forensic and security applications;**
- **Standardization, evaluation and assessment of biometric and forensic applications;**
- **Biometric and Forensic identification and advanced research: What is next?**

The courses will provide a clear and in-depth picture on the state-of-the-art in biometric verification/identification technology, both under the theoretical and scientific point of view as well as in diverse application domains. The lectures will be given by 18 outstanding experts in the field, from both academia and industry.

An advanced feature of this summer school will be some practical sessions to better understand, "hands on", the real potential of today's biometric technologies.

The school is open to about 50 highly qualified, motivated and pre-selected participants. Phd students, post-docs, researchers, forensic examiners, police officers and professionals are encouraged to apply.

For more information: http://biometrics.uniss.it/

The school will be held in conjunction with the International Worskshop on Biometrics and Forensics (IWBF 2018 http://iwbf2018.uniss.it)

EAB Biometric News, January 8, 2018

Majority of European consumers trust organizations using biometrics for online authentication

More than two in three Europeans (68 percent) would trust organizations more if they used biometrics for authentication, according to survey results released Tuesday by Unisys. The survey results indicate broad consumer support for biometric online authentication.

Unisys surveyed 3,500 consumers in seven European countries about their opinions on the use of biometric authentication for online accounts and trust levels in organizations managing and storing their personal data. Their responses show 63 percent believe biometrics are stronger than traditional PIN.

Russia Starts Biometric Database Next Year

by Jake Rudnitsky, 26 December 2017

Russia will get a country-wide biometric database for financial services starting next summer, the central bank said. The system will expand access to banking by letting people open accounts without having to visit a branch and is a key milestone in digitizing financial services, the Bank of Russia said in a statement.

The regulator said that data would only be stored with individuals' consent. Legal changes needed for the system passed this month. State-owned Rostelecom PJSC has been selected to run the database, which will collect personal data including images of faces, voice samples and, eventually, irises and fingerprints. Facial-recognition technology has been gaining consumer acceptance around the world, with Apple Inc.'s latest iPhone using it to unlock the device. In Russia, the authorities and government-linked companies are leading the charge. Moscow claims it has the largest centralized surveillance network in the world, and uses facial-recognition technology to help police the city. Sberbank PJSC, the state-owned lender that holds nearly half of retail deposits in Russia, last month acquired a 25% stake in VisionLabs as a first step toward building a biometric platform to identify people through face, voice and retina recognition technologies.

Rostelecom's board chairman is Sergei Ivanov, a former KGB agent who was President Vladimir Putin's chief of staff until last year and is currently among those sanctioned by the U.S. for Russia's 2014 annexation of Crimea from Ukraine. The law will take effect six months after it is officially published. The database could also be expanded for use by microfinance organizations and government services, the central bank said.

(Source: Google Alerts)

EAB Biometric News, January 8, 2018

Cognitec Brings Unique Video Investigation Features to Face Recognition Product for Law Enforcement

Dresden, Germany; December 13, 2017

Cognitec Systems, the face recognition company, has significantly extended the feature set of its FaceVACS-DBScan product. The latest release combines the company's renowned image database search technology with powerful video inspection tools for a multitude of investigation use cases.

FaceVACS-DBScan LE enables fast import of video footage and detailed investigations of the

extracted facial images. Agents can find known or unknown persons in multiple videos to quickly narrow down suspect investigations. The investigation can reveal, for example, if a suspect was seen in various locations within a set time window, always with the same group of persons, or in one location too many times during the day. With one click, the investigator can add the facial image seen in a video frame to a local database. If a person is already known, the technology can quickly compare the facial image to all connected databases and instantly display a candidate list of possible matches. "Searching through hours of video material continues to be one of the most tedious investigation

tasks for law enforcement professionals," says Alfredo Herrera, Cognitec CEO. "This tool will bring a new level of search automation and efficiency to the investigative workflow."

This product release maintains established features that have been in successful use for years by law enforcement professionals worldwide. Investigators can compare facial images from any source to multi-million image databases and instantly view a match list of the most similar faces. The use of image enhancement tools can improve match results, and side-by-side image inspections allow for precise match evaluation of probe and candidate image.

IDEX advances biometric smartcard deployment, develops remote enrollment process

BiometricUpdate.com, 28 November 2017

IDEX has partnered with security solution provider Feitian to commercialize a dual interface biometric smart card, and also developed a remote enrollment solution for biometric cards, enabling users to conveniently enroll without being physically present in a branch office.

Feitian, the no.1 supplier of user authentication and transaction security for China Online Banking while having its business in over 100 countries, has developed a convenient, secure and low cost contact and contactless smart to be offered to the government ID, access control and payment markets. IDEX and their strategic partner IDEMIA predict that the biometric smart card market could reach 300 million units in 2020 in an investor update earlier this month.

“Having watched the development of biometric technologies in other mass market verticals, we are excited to showcase our leadership in introducing biometrics to our existing leading smart card portfolio,” said Yan Yan, VP of Feitian Technologies Co., Ltd. “We are excited to be working with IDEX on these solutions, as they have clear demonstrable performance and cost advantages to conventional sensing solutions.”

Remote self-enrollment to unlock mass deployment of smart cards

The new process of self-enrollment, as developed by IDEX, addresses a barrier to mass deployment of biometric cards in the payment and security markets. It is secure, low-cost, and requires only a smartcard with a standard secure EMV chip without need for an external computer, internet connection, or smartphone.

“This unique self-enrollment process that we have developed at IDEX is further evidence of our continued focus on delivering innovative and seamless end-to-end solutions for biometric cards. The mass adoption of biometric payment cards not only requires a scalable, low-cost, low-power, ISO form factor fingerprint sensor that works with existing payment terminals, but equally importantly it needs a simple, convenient and mass scalable way of enrolling users accurately and securely,” commented Dr. Hemant Mardia, CEO of IDEX. “Our revolutionary new solution allows customers to enroll their fingerprints using a low number of touches by making clever use of the large capture area of IDEX’s off-chip sensor which reduces the need for accurate positioning of the user’s fingers. This is a major improvement in the simplicity, accuracy and cost of the enrollment process verses solutions available in the market today.”

The patent-pending process is designed for usability across geographies and demographics, and IDEX is working with partners to incorporate it into card payment products to support broad commercial deployment of biometric cards it anticipates in 2018.