September 2013: Volume 1, Edition 1

BIOMETRIC UPDATE.COM

The FBI's Biometrics Program

The FBI is in the midst of a massive project hinging on biometric technology. We talk to some major stakeholders and the FBI.

Page 13

IN THIS ISSUE:

biometrics
EXHIBITION AND CONFERENCE 2013

CONFERENCE

Reduced rates for public sector delegates

Gain practical advice, tips and solutions on the use of biometric technology in a number of applications from more than 45 expert speakers...

Join high-level participants for a rich, case-study based programme on the latest practical applications of biometrics and related technologies.

Register now to hear from the following keynote speakers:

Colonel Barakat Al Kindi, *Section Manager, Systems Development Department, Abu Dhabi Police GHQ, Abu Dhabi, United Arab Emirates*

The UAE e-Border: A successful border management system using three biometrics

---

Rasa Karbauskaite, *Research Officer, Frontex, Poland*

Automated Border Controls (ABC) and the future of border checks

---

Nicole A. Spaun, *Biometrics Program Manager for Headquarters, US Army Europe, Germany*

Speech title to be announced

Andrew Hopkins, *Senior Registration Officer, UNHCR Biometrics Programmes, United Nations High Commission for Refugees, Switzerland*

Speech title to be announced

Joseph Atick, *Identity Counsel International, Director IBIA Cofounder & Director Emeritus, France*

Identity management in a data-centric world

Join the dialogue in our privacy debate session:

Privacy at the cross road: A debate on frameworks

Session led by: Joseph Atick, *Identity Counsel International, Director IBIA Cofounder & Director Emeritus, France*

Panellists: Emilio Mordini, *Professor and Director, Centre for Science, Society and Citizenship, Italy* and Pam Dixon, *Executive Director, World Privacy Forum, USA*

FULL PROGRAMME NOW ONLINE AT:

www.biometrics2013.com

QUEEN ELIZABETH II CONFERENCE CENTRE, WESTMINSTER, LONDON, UK

Conference: 15–17 October 2013 | **Exhibition:** 16–17 October 2013

EXHIBITION

Now in its 16th year

biometrics Live!

FREE EXHIBITION

View the latest in identity management from the following exhibiting companies:

- 3M Security Systems
- Abilma LLC
- Accenture
- AOptix
- Atkins
- Aurora Computer Services Ltd
- Aware, Inc
- Biometric Technology Today
- Borer Data Systems
- CMI-Tech
- Cognitec Systems
- Cross Match Technologies
- Daon
- DERMALOG Identification Systems GmbH
- DigitalPersona Inc
- Facebanx
- FASTCOM Technology SA
- Fujitsu Technology Solutions
- GenKey
- Green Bit S.p.A.
- Hitachi Ltd
- Id3 Technologies
- IEEE Certified Biometrics Professional (CBP) Program
- Iris ID Systems, Inc.
- Lumidigm
- M2SYS Technology
- MODI Modular Digits GmbH
- Morpho
- NEC Corporation
- NexID Biometrics LLC
- secunet Security Networks AG
- Smart Sensors
- Speed Identity AB
- SRI International Sarnoff
- Techshino Europe Technology B.V
- Thales Communications and Security
- Vision-Box
- WCC Smart Search & Match

Exhibition opening hours:

Wednesday 16 October: 09.00–17.30

Thursday 17 October: 09.00–16.00

Organised by: ELSEVIER

In association with: biometric TECHNOLOGY TODAY

SIGN UP FOR FREE VISITOR TICKETS AT

www.biometrics2013.com

LETTER FROM THE EDITOR

As a journalist, I've covered my fair share of breaking news, and in that scenario, there's often a lot of uncertainty around the facts.

The same can be said for the importance of facts to the law enforcement community.

Journalists have little to rely on besides the word of others and their own observations and research, but law enforcement has an important edge in confirming facts: biometrics.

As one of the earliest adopters of biometric technology, law enforcement was an obvious choice as the focus of our very first BiometricUpdate.com digital magazine, and I'm excited by what we've put together.

In developing the content for this issue, I've spoken with many of the people behind some of the most significant technologies on the market, as well as some of the decision-makers behind the implementation of massive biometric objectives for the law enforcement community. I've also taken a close look at the importance of standardized biometric data and the development of these specifications for law enforcement and the industry as a whole.

This issue also includes original research from the Biometrics Research Group, in which research lead Rawlson King crunches the numbers for law enforcement biometrics and gives a high-level look at where the industry is headed.

While law enforcement encompasses an important aspect of the biometric discussion, it's only a small piece of the puzzle. As the editor of this magazine, I look forward to watching and documenting the evolution of this exciting space.

Adam Vrankulj
Editor

LETTER FROM THE PUBLISHER

Welcome to the first issue of Biometric Update Digital Magazine, the definitive online magazine for intelligence and insight into the global biometrics marketplace.

BiometricUpdate.com launched in the summer of 2012, publishing daily industry news, long format features and in depth interviews with market leaders and industry trendsetters. Our comprehensive research, analysis and reporting has established us as the publication of record for biometrics industry participants and consumers.

Drawing on the credibility and authority established from our efforts at ***BiometricUpdate.com***, we're pleased to bring you ***Biometric Update Digital Magazine***, a monthly look at the industry using news synopsis, research, in depth analysis and profiles. We hope these stories will help you adapt new ideas to develop and grow your business.

On behalf of everyone who helped put this issue out, thank you. Thank you also to the advertisers who support our product, and you, the reader, for paying attention, making suggestions and keeping us on our toes.

Drop me a line anytime at **stephen@biometricupdate.com** or find us on **Twitter @BiometricUpdate.**

Stephen Mayhew,
Publisher & CEO

BIOMETRIC UPDATE.COM

September 2013
Volume 1, No. 1

Publisher & CEO	Stephen Mayhew
Editor	Adam Vrankulj
Contributing Editor & Lead Researcher	Rawlson King
Director of Sales	Allison Heather
Art Director	Paul Hirsch

ADVERTISING SALES:

Please contact us at 416-473-8853 or email:
stephen@biometricupdate.com.

EDITORIAL DEPARTMENT:

Please contact us at 416-473-8853 or email news@biometricupdate.com .

Published monthly by
Biometrics Research Group.

6 Wilkins Avenue
Toronto, Ontario, Canada M5A 3C3

www.biometricupdate.com

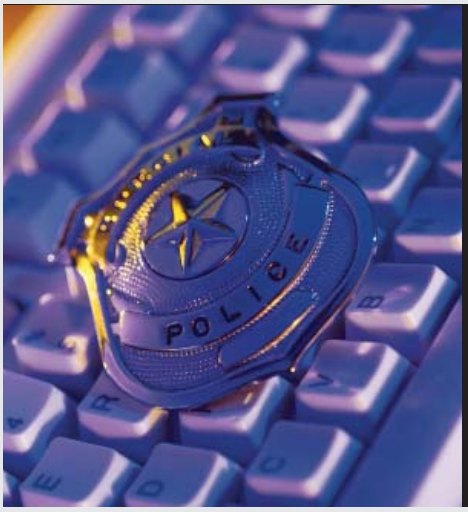
IDENTIFY ANYONE.
ANYTIME. ANYWHERE.

SEEK® Avenger

The benchmark for rapid mobile multi-biometric identification, enrollment, and credential reading. Purpose-built to perform in the harsh and challenging environments of the military, border security, and law enforcement professional.

Get all the facts at www.crossmatch.com/seek-avenger.php

CROSSMATCH®
TECHNOLOGIES



AWARE

BIOMETRICS SOFTWARE

Hardware Abstraction

Fingerprint, Face & Iris

STANDARDS-BASED DATA FORMATTING

VERIFICATION AND IDENTIFICATION

Image Autocapture

Quality and Compliance Assurance

Credential Reading and Personalization

Biometric Services Platform (BioSP™)

SERVICE-ORIENTED APPLICATION SERVER

- Data formatting
- BPEL workflow engine
- Database management
- Transaction management
- Matcher integration
- Quality reporting
- User administration
- Client app configuration

BioComponents™

JAVA APPLETS AND .NET COMPONENTS

- User interfaces
- Capture hardware abstraction
- Autocapture & QA workflow
- Biographics, fingerprint, & face
- Fingerprint card printing and scanning
- Support for .NET or browser applications
- Utilize Aware proven SDKs

Software Development Kits

LIBRARIES, APIS, & SAMPLE APPLICATIONS

- Face and fingerprint autocapture
- Hardware abstraction
- Data formatting and validation
- Fingerprint verification
- Fingerprint card printing and scanning

Client Applications

USER INTERFACES WITH LIBRARIES

- Browser-based enrollment applets
- .NET enrollment with SDKs
- Capture and matching on smart phones
- Drag/drop biometric transaction builder
- OCR-assisted fingerprint card scanning

sales@aware.com | www.aware.com

Bionym launches wearable biometric authentication device

Toronto-based startup Bionym launched its wearable authentication technology, the Nymi, this month. The wearable bracelet recognizes unique ECG patterns and interfaces directly with mobile devices as a replacement for passwords and PINs. Worn on the wrist, the Nymi keeps users authenticated until it's removed. In addition, says the company, the Nymi supports simple, task-specific gesture commands using both motion sensors and proximity detection.

Early Reactions to the iPhone 5S

The rumors were true, and the new iPhone launched with a fingerprint sensor embedded in the home button. Many in the biometrics space see this as the first step towards wider consumer adoption, but a few concerns have been raised: Is Touch ID propriety a good thing, and has Apple priced themselves out of the market? Michael Barrett, president of the FIDO Alliance weighs-in with what he thinks of the new device and what it means for biometrics.

Apple shares sink after iPhone 5S launch

The day after Apple launched its fingerprint-enabled iPhone 5S, shares of the device manufacturer dropped nearly 6%, following a 2% drop the day before This represented a huge loss of market value for the company. What caused this? A lack of enthusiasm for the new device's biometric integration? Interoperability concerns for enterprise clients?

NIST issues update to PIV standard, adds mobile support

NIST issued an update to its standard specification PIV card, with a new FIPS 201-2 publication. This new revision includes a derived PIV credential option for use in mobile devices, optional on-card fingerprint comparison readability, the use of iris alone or in conjunction with fingerprints and the ability to remotely update credentials. NIST had long promised a standard for iris, and now that it's been published, this modality has seen a lot of growth.

Fingerprint Cards sees massive growth in Asian markets: New design wins and massive production orders

It's no surprise that Fingerprint Cards is a major player in consumer biometrics. This past year has been design win after design win, and we're now starting to see the Swedish company's sensors embedded into smartphones in the Asian market. In August, the company nabbed a significant design win for an additional three smartphone models to be launched in Asia from one of its "most distinguished customers." Earlier in the month, Fingerprint Cards announced its largest order to date – for 3.1 million swipe sensors – again for the Asian market.

IDEX gets fingerprint sensor patent license with Apple and AuthenTec

In 2007, IDEX was granted a license to certain key patents owned by UPEK Inc. and they were later assigned toAuthenTec, acquired by Apple last year. Now, Apple and AuthenTec have verified IDEX's licensing agreement through a notice of so-called "recordal" of the license to key patents in the field of fingerprint sensing. According to the company, this puts it in an advantageous position to exploit the mass market potential of this technology for secure ID.

U.S. government spending on big data to grow exponentially

In a recent research article, the Biometrics Research Group, Inc. noted that national security and military applications are driving a large proportion of "Big Data" research spending in the U.S. The group estimates that federal agencies spent approximately $5 billion on big data resources in the 2012 fiscal year. We estimate that annual spending will grow to US$6 billion in 2014 and then to US$8 billion by 2017. Rawlson King's industry analysis projects most of this spending will be directed through the military apparatus of the U.S. government in the near to midterm.

Did this Australian teen just leak the real iPhone 5S fingerprint sensor?

Days before Apple's anticipated iPhone 5S launch, an Australian

teenager who lives in his parents' basement, with supposed access to parts scooped off of Apple assembly lines in China, posted some pretty convincing pictures of what he said was the fingerprint sensor for the new Apple device. Who is this unlikely leaker, and how did he establish such access?

Consumer electronic biometrics market to grow at 40.45% CAGR to 2016

The iPhone 5S has reignited the conversation about biometric integrations in consumer devices, but this is something many players in the industry have been working towards for quite some time. Research recently published by TechNavio confirms this, and finds that the global market for consumer electronic biometrics to grow at a whopping CAGR of 40.45 percent between 2012 and 2016. According to the group, a key factor contributing to this growth is the increase of personal devices for financial transactions.

NIST evaluation gives MorphoTrust iris recognition top marks

The biometric community holds its breath when NIST is about to publish a report. In August, the group announced that MorphoTrust USA's iris identification technologies had proven to be the most accurate and among the fastest, based on recent IREX evaluations. The IREX report studied the performance of iris algorithms on operational databases of over a million iris records.

FINGERPRINTS

Fingerprint Cards brings Takeshi Murakami on board as country manager in Japan

Fingerprint Cards recently appointed Takeshi Murakami as the company's new Country Manager for Japan -- a hotspot for the company's growth as of late. Murakami comes to Fingerprint Cards from AuthenTec, in which he was Senior Sales Manager Japan, responsible for sales into smartphones, tablets, PC and products for all major OEM customers in Japan.

EyeLock appoints Roger An VP of Global Market Development

Roger An recently joined EyeLock as the company's new Vice President of Global Market Development. In this role, An will be responsible for research, analysis and strategic initiatives to further the embedded applications of the technology and to facilitate EyeLock's global expansion, with a heavy focus on Asia. An comes to EyeLock from SK Group – the largest petro chemical and telecommunications conglomerate in South Korea.

Peter Hauser joins VoiceTrust as CCO

VoiceTrust recently announced the addition of Peter Hauser to its team, as the company's new CCO. Hauser is set to lead the global commercial strategy and development from Toronto, Canada and comes with experience and success in commercial development at high-growth technology startups in the speech technology industry, including Scansoft, Lernout & Hauspie and Nuance Communications.

AOptix appoints François Lê as new VP of Global Sales, Communications

François Lê has just been appointed to AOptix as the company's new VP of Global Sales, Communications. Before AOptix, Lê was VP of Global Sales at Network Equipment Technologies, and he has also led sales at Tropos Networks and Aperto Networks.

Fingerprint Cards recruits Jan Johannesson as new VP, strategic planning and portfolio management

Jan Johannesson, who has previously held positions in Ericsson Mobile Platforms and with Northstream AB, has just been brought on board at Fingerprint Cards as the new VP for strategic planning and portfolio management and will work from the company's operations in Sweden.

Putting a face to a name: the growth of facial recognition

By Adam Vrankulj

Facial recognition is without a doubt, one of the fastest growing modalities in biometric identification today. The equipment needed to perform facial recognition is increasingly accessible, accuracy is improving and there have been some recent significant large-scale deployments.

Facial recognition has certainly had its share of media attention in the last few months – starting from the use of facial recognition in trying to identify the Boston Marathon bombers, the Electronic Frontier Foundation's FOIA lawsuit against the FBI for information on its face recognition system, Google's ban of facial recognition apps for Google Glass, Facebook's use of the technology for public profile pictures and disclosures that the Department of Homeland Security's tested a crowd-scanning system called BOSS.

As such, there has been significant academic and research interest in facial recognition, and across the findings are similar: in terms of growth and adoption, this is just the tip of the iceberg.

In July, MorphoTrust USA commissioned Zogby Analytics to perform a survey on support for facial recognition and found that of 1,000 American adults interviewed, a majority supported facial recognition for crime investigation, drivers' license applications and in lieu of passwords to secure personal devices or social media.

Specifically, support for the use of facial recognition for investigating criminal activity was high with 83% of respondents in favor, and as well for drivers' license applications, showing 78% of respondents to be supportive. In regards to securing electronic devices or social media however, enthusiasm decreases, with only 54% of respondents showing support.

33% of respondents said they trust the federal government to use facial recognition the most responsibly, 20% said they trust state governments the most, 8% said they trust-

Putting a face to a name: the growth of facial recognition

By Adam Vrankulj

ed businesses and corporations, 7% said they trust social media and 32% were unsure.

Another poll -- this one from CNN/Time/Orc -- found that although Americans are generally concerned about the government snooping in on their digital communications, they are mostly in favor of facial recognition.

From the report, 59% said they oppose email and cell phone surveillance (up 13% from 2006), but 79% are in favor of using facial recognition at various locations and public events. 81% said they support expanded camera surveillance on streets and in public places.

Based on research from MarketsandMarkets, the global facial recognition market is estimated to grow from $1.92 billion in 2013 to $6.5 billion in 2018, at CAGR of 27.7%. The firm notes that the major driving forces in the market are the growth of the surveillance market, as well as huge amounts of global government spending.

In terms of regions, research argues that North America is poised to be the biggest market for facial recognition, though over the next five years, APAC will experience increased market traction, to become the biggest global market for facial recognition.

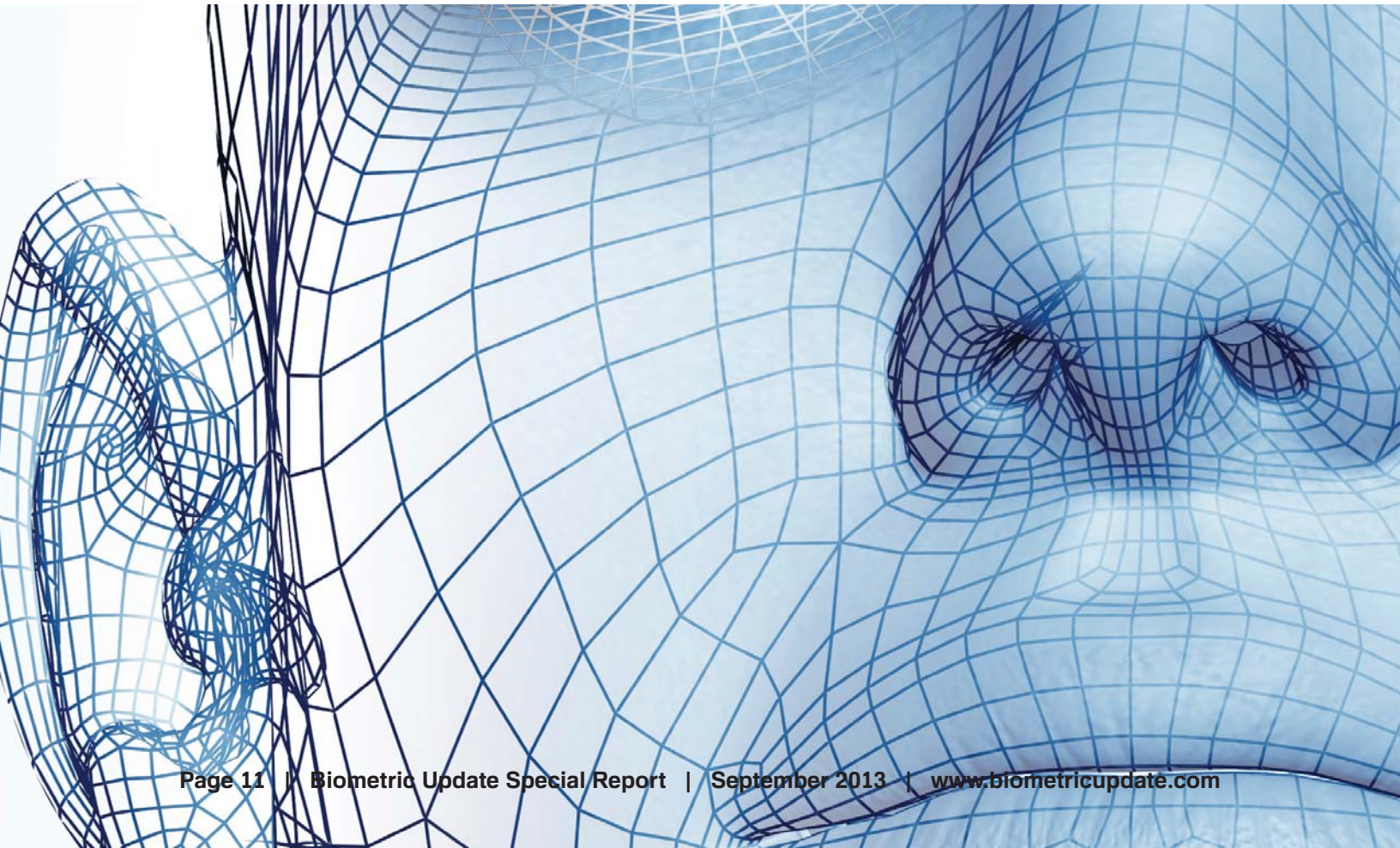
This growth is also fueling other sectors outside of the biometrics sphere.

The video surveillance systems and services market is poised for growth and could reach $36.28 billion by 2018, based on additional research from MarketsandMarkets.

The growth of this market is expected to be higher in North America, though India and China are rapidly driving the Asian-Pacific market.

The market is also likely to witness a large growth in IP video surveillance by 2018.

All signs point to massive growth in this sector, and facial recognition is definitely a technology worth close attention over the next few years.



IDGA
Institute for Defense and Government Advancement

OCTOBER 15 – 18, 2013
WASHINGTON D.C, USA

HOMELAND SECURITY 2013

Delivering Strategic Technologies to America's First Responders

NEW FOR 2013!

Two Lunch Keynotes in the Exhibit Hall

High Profile Speakers include:

- **Robert Mocny,** Director, Office of Biometric Identity Management, **NATIONAL PROTECTION AND PROGRAMS DIRECTORATE**
- **Michael Fisher,** Chief, **U.S BORDER PATROL**
- **Wolfe Tombe,** Chief Technology Officer, **U.S. CUSTOMS AND BORDER PROTECTION**
- **Guy Torres,** Director, Information Technology Contracting, **U.S. CUSTOMS AND BORDER PROTECTION**
- **Daniel Gerstein Ph.D,** Deputy Undersecretary for Science & Technology, **DEPARTMENT OF HOMELAND SECURITY**
- And Many More (see website for speaker full line up)

4 days, 45+ High Profile Speakers, 45 Sessions & 6 Keynotes

Homeland Security 2013 will bring together 1,000's of personnel from **DHS, CBP, FBI, USCG, FEMA** and more to discuss the most pressing issues facing the homeland defense community. In-depth sessions will cover **Land & Maritime Border Security, Cybersecurity & Critical Infrastructure Protection and Disaster Preparedness & Response.** Attend the largest Homeland Security conference of 2013!

FOR MORE INFORMATION OR TO REGISTER FOR YOUR FREE PASS, VISIT:

WWW.HOMELANDSECURITYEXPO.COM

Next Generation Identification: A closer look at the FBI's billion-dollar biometric program

By Adam Vrankulj

Representing a $1.2 billion investment by the U.S. federal government, the FBI's massive Next Generation Identification (NGI) program is a ten-year lifecycle project that hinges on biometric identification technologies and has seen privacy advocates butt heads with law enforcement since its inception.

Split into six "increments," Lockheed Martin was awarded a contract in 2008 to design, build and implement the program on behalf of the FBI, which ultimately aims to enhance the abilities of the agency's aging IAFIS from the mid-nineties.

Increment Zero: Workstation Replacement

Increment zero went live in 2008 and was an overall "tech-refresh" of IAFIS workstations, replacing obsolete hardware with new high-definition monitors, as well as the introduction of modular and replaceable infrastructure for examiners.

Increment One: Ten-print processing

Increment one, which went live in 2011 enhanced the agency's ability to perform back-end processing of ten-print fingerprint data from IAFIS, using algorithms from MorphoTrak, a subsidiary of Morpho. This initially saw a 92.6 percent accuracy rate, though according to Art Ibers, director of criminal justice solutions for Lockheed Martin, the NGI is now 99.6 percent accurate in this regard.

"We had increment one and IAFIS side-by-side for five days, and in those five days, the NGI identified 910 additional matches that the legacy system missed," Ibers said. "We immediately saw value."

This was an important increment in establishing the NGI, as ten-print records have been collected widely for years at local, state and federal levels, so there was a large dataset to begin with. Now, synced at a national level, law enforcement agencies say they're seeing results.

According to Clark Nelson, a senior VP of Marketing at MorphoTrak, the company continues to invest heavily into research and develop-

ment for improving its processing algorithms as even minor adjustments lead to significant improvements when dealing with big data.

"If you think about it, when you're talking about databases of tens of millions – or upwards of hundreds of millions of records – and about thousands of searches per day, an extra tenth of a percent in accuracy can lead to hundreds of new matches," Nelson said. "Even though [our algorithms] are 99 percent accurate already, we strive to go beyond that."

Increment Two: RISC

Increment two was rolled out in August 2011 and saw the establishment of the Repository for Individuals of Special Concern – RISC, as it's known. This database contains the biometric data of known or suspected terrorists, sex offenders, wanted persons and other persons of special interest. It's accessed primarily with a mobile devices and fingerprint data collected from two index fingers. According to the FBI, it gives "situational awareness" to enforcement officers in the field in the 16 U.S states and 689 separate law enforcement agencies with access to the system.

The FBI's Brian Edgell, unit chief of the implementation and transition unit, NGI, says there are roughly 1,200 RISC transactions per day and that a typical use example is when someone can't provide identification to law enforcement or there is reasonable cause to question identification provided. Officers can scan a person's two index fingers to cross-reference with the RISC database and see if it turns up a match. "The FBI maintains this repository and states have access to it," Edgell said. "We're very pleased with how RISC is going."

Increment Three: National Palm Repository and Latent Searches

Increment three, the most recently deployed increment, was first introduced in early May this year with the aim of improving the NGI's latent processing services and establishing a national palm print repository.

According to the FBI, with the new latent processing system, cold cases can be solved more easily and in the four months since launching, it's already paid off. "[Investigators] can register latent prints in the file, and we can cascade new prints coming in every day against that," Edgell said. "If there's a match, we can give leads to latent examiners to who can do a one-to-one comparison to see if they can make an identification."

"Under IAFIS, we only searched composite records, so if someone had six or seven prior arrests, we could only search the compilation of that data, but now we can search all arrest events."

The NGI's third increment also includes the creation of a national palm print database, which combines the existing palm repositories of at least 25 states, Edgell says. This system also employs MorphoTrak processing and matching algorithms. This includes enrolled palm prints, as well as latent prints from crime scenes. "Under the old system, it was very difficult to search the entire file," Edgell said. "Not knowing what part of the hand it was – right or left – is often a challenge. Investigators used to have to search four or five different ways. Now it can be accomplished with a single search of the entire repository."

Increment Four: Facial Recognition and Rap Back

The fourth increment is perhaps the most controversial, as it introduces face as a modality to the NGI. There's been a lot of coverage regarding this deployment and a lot of concern for the scope of the system and it's set to go live next summer.

Reported previously in BiometricUpdate.com, the Electronic Frontier Foundation sued the FBI over access to its facial recognition records based on three Freedom of Information Act requests it made a year ago.

"NGI will result in a massive expansion of government data collection for both criminal and noncriminal purposes," EFF Staff Attorney Jennifer Lynch said. Lynch testified before the U.S. Senate on the privacy implications of facial recognition technology in July last year. "Biometrics programs present critical threats to civil liberties and privacy. Face-recognition technology is among the most alarming new developments, because Americans cannot easily take precautions against the covert, remote, and mass capture of their images."

According to Edgell, there are many of misconceptions around the images that will be used in this deployment.

"We have a true image search of the mugshot repository – that's our gallery," Edgell said. "The photos that we're searching have a corresponding ten-print and an arrest event. We're not searching the internet. We're not searching things like Facebook or social media. We're not searching outside entities like passports or the DMV."

"There are a lot of things on network television that lend themselves to the notion that the FBI does more than that, or that law enforcement does more than that, and it's just not based upon fact. Certainly, technology would enable us to do other things, but authority today does not. We stay within our legal authority and operate within it."

The FBI offers a free facial recognition toolbox to law enforcement agencies to cross-reference mugshot material, and the number of agencies using this system is increasing.

"Today we have about 16 million usable mugshots in the repository and correspondingly, we have approximately 75 million criminal history records in the repository, so there's a significant gap between the number of fingerprints we're searching and the number of mugshots, but that number's increasing much like our palm prints.," Edgell tells me. "We're in an effort now

because we had a place to store the mugshots, but no technical ability or business process that allowed for automated searching. Now we do."

The second aspect of this fourth increment is something the agency is calling "Rap Back," which offers the continuous monitoring of people in "positions of trust." Examples include bank tellers, teachers and people that work with the elderly. There are 30 states today that have laws requiring ten-print background checks for these people and these are typically renewed every five years.

"We're now able to take these records and retain them to cascade against inbound arrest records, so that if someone who holds a position of trust goes out and commits a crime in another state, within a 24-hour period we can notify the state who then notifies the granting authority. They determine whether that person is able to still hold that position or not. The FBI only notifies the state or local agency of an arrest event, the adjudication and, if any, disciplinary action is determined by appropriate authorities," Edgell said.

Before Rap Back, Edgell says that infractions that occur out of state could be missed until another background check is performed five years down the line.

Background checks won't be the only use for the Rap Back program, though. The FBI does have a criminal justice intent in mind for this program as well. In particular, this pertains to people released from prison who are still under correctional supervision. If these people go out and get arrested – in a different state, for example – the Rap Back system would immediately inform supervising authorities who could determine disciplinary action.

Increment Five: Iris Recognition

Increment five is a pilot test of iris recognition and its set to being soon.

"People in criminal justice who manage people are seeing good utility in iris, so we're doing a pilot with several of the big agencies or states that are doing that around the country and then we'll go back to [Office of Management and Budget Affairs at the White House] with our findings if we want to operationalize, because we'll have to request additional funding to do it, but that gets underway later this month," Edgell said.

There's been a lot of focus on iris recognition as of late, and its potential addition to the NGI is unsurprising.

Earlier this year, NIST delivered a new publication for Personal Identity Verification (PIV) cards, which added support for iris images.

During a tense congressional subcommittee hearing in June, Charles Romine, the director of the NIST Information Technology Laboratory promised a standard for iris images in federal identity cards, as the committee's chair Rep. John Mica was adamant the agency be held to account for this new standard, which had reportedly been delayed many times in the past. Now that the standard has been delivered, this storm has passed.

NIST has also recently published a new IREX study, which found that iris is a stable biometric modality, not affected over time by aging eyes.

Currently, many correctional facilities throughout the United States collect iris information and have been active adopters of this technology, not only for inmate identification, but also as a way to perform access control to different sections of prisons without the need to unshackle enrolled and previously-approved prisoners.

Edgell says this is a compelling dataset, as everyone in prison has been arrested, so the data has already been collected and is within reach of the agency. Iris is also a preferred modality for many Homeland Security and Defense Department objectives -- some of which include arrest events. According to Edgell, this could also form part of the usable iris dataset for the NGI, but at this point nothing has been set in stone and data from immigration programs and other data collection efforts would not be included, unless someone's been arrested – in which case it could be fair game for the FBI.

Increment Six: Another Tech Refresh

The final increment of the NGI – the sixth – which will encompass the final two to three years of the project, is another tech refresh to ensure all software and hardware used in the program is up to date and can avoid quick obsolescence.

Mentioned earlier, privacy has been a major concern surrounding the NGI program, but according to Edgell, little of what the program encompasses is new – only the technology being used is.

"NGI did not require the creation of any new authority for the FBI. The FBI had all the authority to do everything I've already described. We just didn't have the technology to do it or the business process to go along with it, so now we are matching up to our authorities to do these things."

Edgell is also adamant to point out that there is a crucial distinction to be made between what the FBI maintains and what the FBI searches. For example, says Edgell, ten-fingerprint searching with the mobile ID system for RISC illustrates this point.

"The only thing we have is a piece of metadata that we retain that says we received a search at a certain time, from an agency, and what the response was. The only way we would alter the criminal history repository is if [the officer] who affected the arrest, took the individual into custody, conducted a live scan and submitted a booking to the criminal history repository."

So far, says Edgell, the NGI is "on schedule, within budget and within scope."

The face recognition company

Cognitec develops market-leading face recognition technologies for enterprise and government customers around the world.

Face recognition technologies are constantly evolving in response to new applications and quickly changing biometric markets.

Cognitec's leading-edge products efficiently implement the different processes involved in today's identity management systems using facial data:

- identity verification
- duplicate check
- background check
- management of identity information
- real-time identification in video streams
- acquisition of biometric facial photographs

At the same time, Cognitec's products enable new commercial and consumer applications using facial data:

- analyzing people flow by count, age, gender and other measures
- recognizing VIP customers
- enabling digital signs to tailor advertisements
- logging in to computers, phones and banking machines
- indexing and sorting photographs in digital photo albums
- automotive applications for convenience and safety
- allowing humanoid/service robots to recognize faces and interact with people

Biometric performance has always been the major focus of Cognitec's research and development.

Continued tests of government authorities and industry have validated Cognitec's leadership position within the face recognition market since 2002, resulting in a track record of successful reference projects worldwide.

Biometrics and Law Enforcement Research Report

This report provides a brief overview of the market size and biometric technologies available for the law enforcement market in the United States.

Rawlson O`Neil King
Lead Researcher, Biometrics Research Group, Inc.

TABLE OF CONTENTS

Research Methodology

Biometrics Research Group, Inc. uses a combination of primary and secondary research methodologies to compile the necessary information for its research projections.

The conclusions drawn are based on our best judgment of exhibited trends, the expected direction the industry may follow, and consideration of a host of industry drivers, restraints, and challenges that represent the possibility for such trends to occur over a specific time frame. All supporting analyses and data are provided to the best of ability.

Primary Research

Biometrics Research Group, Inc. conducts interviews with technology providers, clients, and other organizations, as well as stakeholders in each of the technology segments, standards organizations, privacy commissions, and other influential agencies. To provide balance to these interviews, industry thought leaders who track the implementation of the biometric technologies are also interviewed to get their perspective on the issues of market acceptance and future direction of the industry.

Biometrics Research Group, Inc. also applies its own proprietary micro- and macroeconomic modeling using a regression analysis methodology to determine the size of biometric and related-industry marketplaces. Using databases of both publicly and privately-available financial data, Biometrics Research Group works to project market size and market potential, in the context of the global economic marketplace, using proven econometric models.

Secondary Research

Biometrics Research Group, Inc. also draws upon secondary research which includes published sources such as those from government bodies, think tanks, industry associations, internet sources, and Biometrics Research Group, Inc.'s own repository of news items. This information was used to enrich and externalize the primary data. Data sources are cited where applicable.

Market Synopsis

The law enforcement market includes the use of biometrics to identify or verify the identity of individuals (1) apprehended or incarcerated because of criminal activity, (2) suspected of criminal activity, or (3) whose movement is restricted as a result of criminal activity. Biometrics may be used to identify non-cooperative or unknown subjects, to ensure that the correct inmates are released, or to verify that users under home arrest are in compliance.

Biometrics Research Group, Inc. defines biometrics as a physical trait or pattern which is unique to every individual. It is often used to verify and authenticate a person's identity that is enrolled into a system. Biometric patterns can be anything from fingerprints, iris scans, facial recognition or even voice recognition.

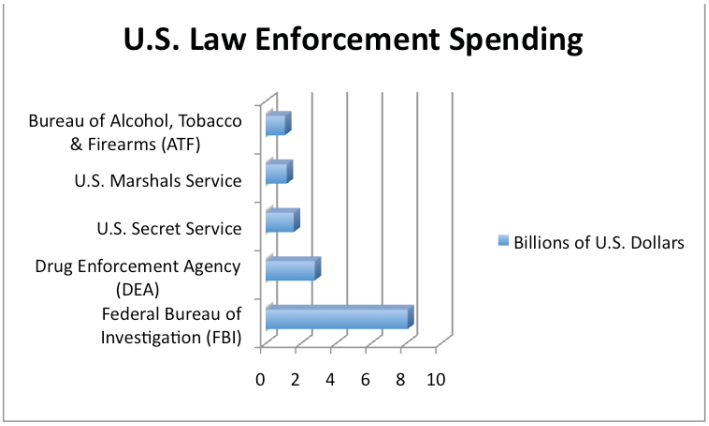
The law enforcement market is characterized by the widespread use of biometric technologies, including automated fingerprint identification technology, voice, iris, and facial recognition, implemented at the state and federal levels across the United States and increasingly around the world.

Biometrics Research Group, Inc. expects that major investment by law enforcement in the usage of biometrics will occur through the introduction of multi-modal biometrics to existing automated fingerprint identification database and through the wide spread deployment of surveillance systems that leverage "Big Data" over the next decade.

Market Size

The U.S. Government spent US$14.8 billion on the Federal Bureau of Investigation (FBI), the Drug Enforcement Agency (DEA), the U.S. Secret Service, the U.S. Marshals Service, and the Bureau of Alcohol, Tobacco and Firearms (ATF) combined in fiscal year 2012. Local U.S. governments spent approximately US$100 billion generally on total police services in fiscal year 2012.

In terms of biometric technologies, automated fingerprint identification systems (AFIS) and fingerprint biometric technologies accounted for the greatest share of the biometrics spending in the U.S. law enforcement sector, followed by face, iris, facial, and voice recognition biometric technologies.



Biometrics Research Group, Inc. estimates that in fiscal year 2012, automated fingerprint identification systems accounted for US$3 billion in law enforcement spending, while combined spending on face, iris, facial and voice recognition accounted for approximately $1 billion. Investments in newly unveiled "rapid DNA" technologies only totaled US$50 million in 2012, but the Biometrics Research Group projects fast growth (US$250 million in rapid DNA spending by 2015) as governments work to reduce their backlogs of unanalyzed DNA samples and rush to process DNA samples in the field.

In 2012, Biometrics Research Group Inc. estimated that the U.S. Government spent at least US$450 million per annum on pure biometric research. With the advent of new technologies such as rapid DNA and greater investment in facial recognition technologies, along with investments in "Big Data" systems, Biometrics Research Group now estimates that U.S. Government spending is at least US$700 million per annum on basic biometric research, despite severe spending cuts caused by budget sequestration.

Biometrics Research Group, Inc. expects greater investment by the U.S. Government to expand its automated fingerprint identification system to include multi-modal biometrics, which will include face, iris, facial and voice recognition. Our firm also expects

greater use of rapid DNA and "meta-data" surveillance.

Automated Fingerprint Identification (AFIS)
Automated fingerprint identification is the process of automatically matching one or many unknown fingerprints against a database of known and unknown prints. Automated fingerprint identification systems are primarily used by law enforcement agencies for criminal identification initiatives, the most important of which include identifying a person suspected of committing a crime or linking a suspect to other unsolved crimes.

An Automated Fingerprint Identification System (AFIS) is a biometric identification (ID) methodology that uses digital imaging technology to obtain, store, and analyze fingerprint data. The AFIS was originally used by the U.S. Federal Bureau of Investigation (FBI) in criminal cases. Lately, it has gained favor for general identification and fraud prevention.

Fingerprinting, as a form of personal identification, is a refined methodology that is proven in practice and accepted in courts of law. AFIS itself has been around for more than 25 years. Recently, a more advanced form of AFIS uses a process called plain-impression live scanning.

Several vendors offer automated fingerprint identification equipment and programs including 3M Cogent and Safran.

With greater frequency in recent years, automated fingerprint identification systems have been used in large-scale civil identification projects. The chief purpose of a civil fingerprint identifications system is to prevent multiple enrollments in an electoral, welfare, driver licensing, or similar system. Another benefit of a civil fingerprint identifications system is its use in background checks for job applicants for highly sensitive posts and educational personnel who have close contact with children.

The AFIS market is mature by biometric standards, having already reached a substantial percentage of its potential deployment areas. Developments in the AFIS market include new portable devices tied to central databases for field suspect identification.

The Integrated Automated Fingerprint Identification System (IAFIS) holds all fingerprint sets collected in the United States, and is managed by the FBI. Launched in 1999, the FBI's database is used by federal and local law enforcement agencies to solve and prevent crime and catch criminals and terrorists. IAFIS provides automated fingerprint search capabilities, latent search capability, electronic image storage, and electronic exchange of fingerprints and responses.

IAFIS is the largest biometric database in the world, housing the fingerprints and criminal histories for more than 70 million subjects in the criminal master file, along with more than 34 million civil prints. Included in its criminal database are fingerprints from 73,000 known and suspected terrorists processed by the U.S. or by international law enforcement agencies.

Many states also have their own AFIS. AFISes have capabilities such as latent searching, electronic image storage, and electronic exchange of fingerprints and responses.

Many other countries and regions, including Canada, the European Union, the United Kingdom, Israel, Pakistan, Argentina, Turkey, Morocco, Italy, Chile, Venezuela, Australia, Denmark, the International Criminal Police Organization, and various states, provinces, and local administrative regions have their own systems, which are used for a variety of purposes, including criminal identification, applicant background checks, receipt of benefits, and receipt of credentials, such as passports.

European police agencies are now required by European Union legislation to open their AFISes to each other to improve information sharing to combat terrorism and investigations of cross-border crime.

The U.S. Government is leading innovation in the AFIS field by proposing to add multi-modal biometrics, including face, iris, facial, voice and even tattoo recognition to its existing Integrated Automated Fingerprint

Identification System.

Multi-modal Biometrics (Face, Iris, Facial and Voice Recognition)
In 2012, the U.S. Federal Bureau of Investigation decided to widen its Integrated Automated Fingerprint Identification System (IAFIS) to become multi-modal.

As part of a US$1 billion update to the national fingerprint database in the United States, the Federal Bureau of Investigation has begun rolling out facial recognition to identify criminals.

Facial recognition is a computer-based application system for automatically identifying or verifying a person from a digital image or a video frame from a video source by comparing selected facial features against a facial database.

The implementation of new biometric identifiers in the FBI's Integrated Automated Fingerprint Identification System is part of the FBI's new "Next Generation Identification" program effort. The program is designed to advance the bureau's biometric identification services, providing an incremental replacement of its current integrated automated fingerprint identification capabilities with a multi-modal biometric database.

According to the FBI, the future of identification systems is currently progressing beyond the dependency on a uni-modal, fingerprint biometric identifier towards other multi-modal biometrics, including voice, iris and facial recognition.

Voice recognition systems, broadly as known as 'voice biometrics', is a biometric modality that uses an individual's voice for recognition purposes. It is a different technology than "speech recognition", which recognizes words as they are articulated, which is not a biometric. The speaker recognition process relies on features influenced by both the physical structure of an individual's vocal tract and the behavioral characteristics of the individual.

Iris recognition is the process of recognizing a person by analyzing the random pattern of the iris. The iris is a muscle within the eye that regulates the size of the pupil, controlling the amount of light that enters the eye. It is the colored portion of the eye with coloring based on the amount of melatonin pigment within the muscle.

The Next Generation Identification program will be designed to advance the integration strategies and indexing of additional biometric data that will provide the framework for a future multi-modal system that will facilitate biometric fusion identification techniques.

The framework will be expandable, scalable, and flexible to accommodate new technologies and biometric standards, and will be interoperable with existing systems. Once developed and implemented, the new FBI biometric initiatives and multi-modal functionality will promote a high level of information sharing, support interoperability, and provide a foundation for using multiple biometrics for positive identification.

The existing database currently consists of iris scans and DNA samples, but the newly updated database will also contain tattoos. Another proposed element of an updated database includes an image matching service. Under such a service, images of a person of interest from security cameras or photos accessed from sources such as the Internet could be compared against a national repository of images held by the FBI.

The FBI will also expand its capability to accept, store, and search palm print submissions from local, state, and federal law enforcement and criminal justice agencies. The bureau's new system will provide a centralized repository for palm print data that can be accessed nationwide, providing local police with an additional tool to solve crimes.

The objective of the program is to reduce terrorist and criminal activities by improving and expand-

ing biometric identification and criminal history information services through research, evaluation, and implementation of advanced technology that would be made widely available to local law enforcement agencies.

Lockheed Martin Transportation and Security Solutions will undertake implementation of the project. The multi-million dollar contract, which was awarded after a full and open competition, will consist of a base year and the potential for up to nine option years. A roster of other contractors will also augment the project.

DNA

DNA is generally used to solve crimes in one of two ways. In cases where a suspect is identified, a sample of that person's DNA can be compared to evidence from the crime scene. The results of this comparison may help establish whether the suspect committed the crime. In cases where a suspect has not yet been identified, biological evidence from the crime scene can be analyzed and compared to offender profiles in DNA databases to help identify the perpetrator. Crime scene evidence can also be linked to other crime scenes through the use of DNA databases.

Among various possible biometric modalities, DNA provides the most reliable personal identification. It is intrinsically digital, and does not change during a person's life or at the time of their death.

Deoxyribonucleic acid is a molecule that encodes the genetic instructions used in the development and functioning of all known living organisms and many viruses.

In the human body, DNA, which can be thought of as the blueprint of biological design, is folded inside the nucleus of each cell. It is estimated that the human body is composed of approximately 60 trillion cells.

DNA are nucleic acids. Alongside proteins, they compose the three major "macro-molecules" essential for all known forms of life.

DNA is a polymer, and is composed of nucleotide units that each has three parts: a base, a sugar, and a phosphate. The bases are adenine, guanine, cytosine and thymine, abbreviated A, G, C and T, respectively. These four letters represent the informational content in each nucleotide unit.

DNA also has a backbone made of alternating sugars (deoxyribose) and groups of andphosphate material (which is related to phosphoric acid), with the nucleobases (G, A, T, C) attached to the sugars.

DNA is well-suited for biological information storage, since the DNA backbone is resistant to cleavage and the double-stranded structure provides the molecule with a built-in duplicate of the encoded information.

Variations in the nucleotide sequence bring about biological diversity, not only among human beings but among all living creatures. Phosphate and sugar form the backbone structure of the DNA molecule. Within a cell, DNA exists in a double-stranded form, which can be visualized as two anti-parallel strands that spiral around each other in the form of a double helix.

DNA is an excellent biometric identifier because it unique to each individual. Although 99.9 percent of human DNA sequences are the same in every person, enough of the DNA is different to distinguish one individual from another, unless they are monozygotic twins.

Biometrics use methods for unique recognition of humans based upon one or more intrinsic physical or behavioral traits. DNA can be classified as one of humanity's most intrinsic features. As a result, DNA profiling is often used for criminal investigations.

The DNA profiling technique was first used in 1984 and devised by Alec Jeffreys at the University of Leicester in England. The technique is now the basis of several national DNA databases used for criminal justice. Dr. Jeffreys's profiling technique was made commercially available in 1987, when Imperial Chemical Industries (ICI) started a blood-testing center in England.

DNA profiling begins with a sample of an individual's DNA (typically called a "reference sample"). The most desirable method of collecting a reference sample is the use of a buccal swab, a non-invasive collection of DNA cells from a person's cheek, which reduces the possibility of contamination.

When this is not available, other methods may be used to collect DNA, including: a sample of blood, saliva, semen, or other appropriate fluid or tissue from personal items such as a toothbrush or razor. Stored samples such as banked sperm or biopsy tissue can also be used. Samples obtained from biological relatives can also provide an indication of an individual's profile, as can human remains, which had been previously profiled.

A reference sample is then analyzed to create the individual's DNA profile using one of a number of techniques, which include RFLP, PCR and STR analysis, as well as Y-chromosome and mitochondrial analysis, along with AmpFLP and DNA family relationship analysis.

The DNA profile is then compared against another sample to determine whether there is a genetic match. Such profiling is often used to solve high-impact and high-profile crimes, such as murder and rape. The technology has be popularized in the media, by highly-rated dramas such as the CSI: Crime Scene Investigation television franchise.

DNA evidence is generally linked to DNA offender profiles through DNA databases. In the late 1980s, the federal government laid the groundwork for a system of national, state, and local DNA databases for the storage and exchange of DNA profiles. This system, called the Combined DNA Index System (CODIS), maintains DNA profiles obtained under the federal, state, and local systems in a set of databases that are available to law enforcement agencies across the country for law enforcement purposes. CODIS can compare crime scene evidence to a database of DNA profiles obtained from convicted offenders. CODIS can also link DNA evidence obtained from different crime scenes, thereby identifying serial criminals.

In order to take advantage of the investigative potential of CODIS, in the late 1980s and early 1990s, states began passing laws requiring offenders convicted of certain offenses to provide DNA samples. Currently all 50 states and the federal government have laws requiring that DNA samples be collected from some categories of offenders.

When used to its full potential, DNA evidence solves and prevents the most serious violent crimes. However, the current federal and state DNA collection and analysis system needs improvement. In many instances, public crime labs are overwhelmed by backlogs of unanalyzed DNA samples. In addition, these labs may be ill-equipped to handle the increasing influx of DNA samples and evidence. The problems of backlogs and lack of up-to-date technology result in significant delays in the administration of justice. In order to clear out the backlog, new technological advances are now being employed. New portable rapid DNA machines are being designed for use by law enforcement officers in booking stations to initiate DNA collection of arrested individuals in order to expedite analysis.

With several government agencies in the United States and Europe incentivizing development efforts, the first generation of "rapid DNA" prototypes systems have been made available for evaluation.

Lockheed Martin and ZyGEM Corp. Ltd. released a version of their rapid DNA analysis platform in 2012 designed to simplify and speed DNA analysis for human identity testing. Pre-production units of the platform will be released this summer to select customers in the forensic, homeland security and intelligence communities.

With the successful development of a fully-integrated cartridge device, new rapid DNA platforms have the potential to transform today's existing DNA identification process from one that takes a great deal of training, sophisticated equipment and time into a far simpler, more affordable process that can be performed in the lab or field in under 90 minutes.

Lockheed's platform leverages the latest in microfluidic research and development to accelerate the DNA identification process, essentially building a laboratory on a small, single chip that reduces the processing steps and time needed for analysis.

Lockheed is targeting its rapid DNA system to assist the U.S. Department of Justice's backlog of DNA requests. It is expected that the technology will also be of interest to law enforcement agencies in the United States and the United Kingdom.

Recently, field-testing also occurred of another mobile, rapid DNA lab service that yielded full DNA profiles to a Florida police department in two hours or less. RapidHIT, the system developed by IntegenX Inc. and Promega Corporation will allow law enforcement to produce DNA profiles for human identification from mouth swabs and other human samples.

The RapidHIT service has been described as a breakthrough sample-to-profile biometric system because it allows DNA analysis at the point of collection, such as an arrest or detention, setting a new standard in the usage of DNA profiles as an actionable biometric.

By contrast, human DNA samples currently must be transported or shipped to laboratories that rely on highly trained technicians using multiple instruments for analyses taking 10 to14 hours, with access to results delayed up to 30 days or more.

Already tested in multiple environments including field, office, and laboratory locations, RapidHIT is expected to launch in the U.S. and abroad soon.

Surveillance and Big Data

Surveillance has become a major growth area for law enforcement applications. Systems are available that can compare facial images acquired through surveillance cameras to hotlists of known offenders. The potential for law enforcement-related surveillance applications is substantial. As a consequence, surveillance systems have been marketed, sold and licensed in the United States and around the world for incorporation into existing video capture systems.

These new systems leverage "Big Data", which is typically defined as a collection of data sets so large and complex that it becomes difficult to process using on-hand database management tools or traditional data processing applications. As a consequence, Big Data utilizes massive computer resources that are both physically available and in the cloud to run complex algorithms on millions of data points (known as "meta-data"), in order to create predictive criminal behaviour profiles.

In 2012, Microsoft began to work with the City of New York on developing a Big Data surveillance system entitled "Domain Awareness". The new system will be designed to collate data from over 3,000 closed-circuit television cameras from Lower and Midtown Manhattan. Other data that will be fed into the system will include information from 2,600 mobile radiation detectors distributed to New York Police Department (NYPD) officers on patrol, and 100 license plate readers that are installed at bridges, tunnels, streets, and on city police cars, along with databases of crime patterns

along with live data from 911 calls and police radios. The system will function provide all information visually and geographically, in a chronological context. The system will draw heavily upon facial scan technology.

Tampa police also used "behavior recognition" surveillance cameras and specialized software at the Republican National Convention last year. The software, designed by BRS Labs, used artificial intelligence that can connect to existing video surveillance systems to detect potential threats. The system, entitled "AISight" was designed to learn on its own, about the environment and objects it observes in each surveillance camera's field of view. Since the way the software learns is perpetual, AISight understands which activities commonly occur in any particular scene, bringing attention to objects or behaviors that are out of the ordinary through real-time alert notification. It begins autonomously learning about every environment it observes from the moment it is connected to a video network.

After the software has been started, it connects to the video network and begins to monitor the unique environment and activities for each individual camera. Each camera view is stored as a separate memory. Elements that are always present in the environment become part of the "background." Objects that enter the field of view are analyzed based on their appearance, classification and interaction within its environment and other objects. AISight analyzes the structures, sizes, shapes, locations, velocities, accelerations, paths of objects and other characteristics of all objects within the scene and forms memories about them. It also records timestamps for these events and remembers during what times of day or days of the week events most frequently occur.

Whenever AISight observes objects and behaviors, it compares these events to its current memories. The less frequently it has observed an event in the past, the weaker its memory will be about the event and the more unusual it will deem the current activity. Unusual activity is immediately reported to security personnel to enable a proactive response to potential threats, but normal activity is ignored. And even when AISight has learned to ignore certain activities, it can still be told to alert security personnel of those activities regardless of how often they occur, if needed.

The most notable and widely reported case of wide area network surveillance is that of former senior U.S. intelligence officials, who have reportedly created a detailed domestic surveillance system that leverages a network of security cameras and facial recognition software.

Entitled TrapWire, the system digitally records video at surveillance points in major cities and landmarks across the United States and instantaneously delivers intelligence information to a fortified central database center at an undisclosed location.

TrapWire describes itself as a risk mitigation technology and services company that designs, builds and markets software products intended to prevent terrorist and other criminal attacks directed against critical infrastructure, key assets and personnel.

The TrapWire software system, designed by a subsidiary of Abraxas, a Virginia-based company that is staffed by the elite of the U.S. intelligence community, is built to provide a simple yet powerful means of collecting and recording suspicious activity reports. Once a suspicious activity is entered into the TrapWire system, it is analyzed and compared with data entered from other areas within a network for the purpose of identifying patterns of behavior that are indicative of pre-attack planning.

The TrapWire system includes a variety of features and components that are configured and delivered based on the specific needs of clients within the public and private sector. Abraxas offers variants of the system for critical infrastructure protection,

community surveillance, and information sharing systems for U.S. law enforcement.

Current facial scan systems do have limitations, however. The nature of surveillance applications is such that only a very small percentage of individuals are likely to be correctly identified. Variables such as lighting, camera angle, image quality, distance of the subject from the camera, and the size of the watch list database, ensure that surveillance an extremely difficult application. A large number of users may be incorrectly identified in an effort to find wanted suspects, while the suspects themselves may well go unidentified. As a result, a large amount of private sector research is being conducted to improve the technology.

One of the leaders in developing solutions to the problem of poor facial recognition from video surveillance is Animetrics, a developer of advanced 3-D facial recognition and identity management solutions. The firm has developed a cloud-based solution entitled ID-Ready, a subscription-based online service for smaller law enforcement departments. The service takes a grainy, partial view, angulated 2-D facial image, applies 2-D to 3-D algorithms and corrects the pose of the face, and makes it ID-Ready for most any facial recognition system. Most facial recognition systems require photos be a frontal view of a face in order to make a positive match. However, most photos studied by law enforcement are of faces that are rotated, "off pose" and are captured by low resolution video security cameras or long distance telephoto surveillance cameras. This system allows law enforcement agencies to make matches with angulated images without heavy software or hardware investments. Law enforcement agencies are able to access the information through simple broadband connections.

Mug Shots

Facial recognition is also used to compare mug shots against databases of known or wanted offenders, leveraging non-proprietary equipment for image capture.

Mug shot searching is a near-ideal use of facial-scan: It does not involve the introduction of new acquisition devices, it automates what is currently a manual process, it occurs within a controlled acquisition environment, it performs rapid searches, and it is not relied upon to provide 100 percent accuracy.

Corrections

Fingerprint recognition and iris-scan technologies are used in corrections applications to process incoming and outgoing inmates. While finger-scan is widely deployed in these environments, iris-scan deployments are less prominent. Prisons in Pennsylvania, New York, and Florida use iris-scan technology to verify the identity of convicts before release. This system is designed to avoid the possibility of accidentally releasing or granting privileges to the wrong prisoner as the result of fraudulent identity claims. Other implementations in correctional facilities enroll visitors to ensure that people leaving the facilities are visitors, not inmates. Corrections environments are challenging due to the potential for encountering a highly uncooperative user population.

Probation and Home Arrest

In addition to arrest and incarceration, biometrics are used for post-release programs to ensure compliance with probation, parole, and home detention terms. While outside of facilities, people can be difficult to track, and such tracking can require extensive manpower and administrative resources. Typical methods of tracking, such as scheduled visits by officers or telephone calls, can result in a long delay between the time that a tracked individual disappears and the point at which the authorities become aware that he or she is missing.

Voice recognition is an attractive solution to this problem: In order to verify that an individual is at home while under house arrest, an automatic system telephones the person at regular intervals. Using a challenge-and-response recorded dialogue, the system automatically verifies that the individual

is at home through voice-scan. If the voice answering the phone does not match the voice template, or if no one answers the phone, the system immediately alerts officers so that appropriate action may be taken. Hand-scan technology has also been used in kiosk-based systems to verify the identity of probationary offenders, reducing the burden on probation officers.

Societal & Market Challenges

Due to the societal and political preoccupation with safety and public order in the United States, the Biometrics Research Group expects continued spending on biometric technologies to increase, in order to aid law enforcement agencies. Increased spending will lead to continued innovation in areas such as facial recognition, rapid DNA analysis and especially in surveillance and Big Data systems. The challenge that the Biometrics Research Group foresees surrounding the emerging of new technologies will be legal rather than economic. In February 2013, the Biometric Research Group, Inc. told the Canadian Postmedia newspaper chain that the biggest risk it has perceived is that while government surveillance can be employed to mitigate crime, Big Data surveillance operations tend not to be inhibited by warrants driven by "probable cause" or constrained by illegal "search and seizure" rules. As a result, profiles can be assembled on law-abiding citizens using hundreds of thousands of points of meta-data, without any court-approved authorization. Greater security will be achieved, but accompanied by the loss of privacy and constitutional protections.

More Research Notes Available on BiometricUpdate.com

U.S. Government Spending on Big Data to Grow Exponentially

Biometrics Research Group, Inc. has observed that national security and military applications are driving a large proportion of "Big Data" research spending.

Genetic testing will drive new luxury advertising market

Biometric Research Group, Inc. expects that genetically-driven personal advertising marketplaces will emerge and become a popular luxury offering to consumers in advanced economies by 2020.

Eye tracking and gesture will control future mobile devices

Biometrics Research Group, Inc. expects that technologies that track eye and gesture movements will play a large role in future mobile applications and devices.

Next round of smartphones to incorporate biometrics

Biometrics Research Group, Inc. expects that biometrics will become integrated within a wide number of mobile devices in the near future.

Biorhythm-based consumer electronics to become mainstream

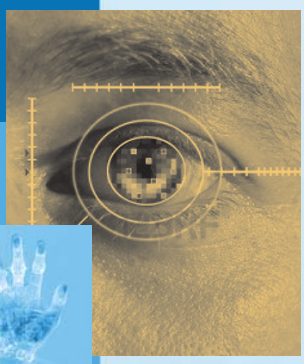
Biometrics Research Group, Inc. estimates that wearable health and fitness sensors will exceed 40 million shipments by 2015.

IDGA
Institute for Defense and Government Advancement

BIOMETRICS FOR GOVERNMENT AND NATIONAL SECURITY

JANUARY 27-29, 2014 | WASHINGTON D.C

WWW.BIOMETRICSEVENT.COM



Biometrics will continue to play an influential role in homeland security and law enforcement. The Defense Biometrics and Forensics Agency, the DoD's branch for biometrics, has announced continuous funding and interest through to FY 2015.

Don't miss IDGA's largest Biometrics event to date with over 35 sessions dedicated to the current and future trends of the biometrics community. Learn from key decision makers and biometric technology experts on the future of securing our war fighters, citizens, government employees, and borders.

HIGH PROFILE SPEAKERS INCLUDE:

- **ROBERT MOCNY**
  Director, Office of Biometric Identity Management
  National Protection and Programs Directorate
- **JAMES LOUDERMILK**
  Senior Level Technologist
  FBI Science and Technology Branch
- **DALTON JONES**
  Biometric ID Intelligence Executive
  DIA
- **WALTER HAMILTON**
  Vice Chairman
  International Biometricas and Identification Association
- **JOHN BOYD**
  Director, Defense Biometrics and Forensics
  Office of the Secretary of Defense
- **ANY MANY MORE**

ATTENDEES WILL LEARN:

- **STANDARDS FOR BIOMETRICS**
- **BIOMETRICS FOR NEW APPLICATIONS**
- **THE LATEST IN BIOMETRIC TECHNOLOGIES (FINGERPRINT, RETINA, FACE)**
- **MOBILE BIOMETRICS**

FOR MORE INFORMATION, OR TO REGISTER VISIT
WWW.BIOMETRICSEVENT.COM

Finding common ground: Standards development in biometrics

By Adam Vrankulj

Biometrics is a definitive science. There is little tolerance for grey area – things are either a match, or they aren't. Practically speaking, that's a best case scenario and is something the industry grows closer to every day. Identification technologies are being implemented so widely today that standardization is becoming increasingly important across the board.

Law enforcement and border control benefit from standards so they can share information. Interoperability is important here, and there are some long-established standards and industry bodies that work to ensure everyone is on the same page and that biometric systems work together.

Consumer biometrics on the other hand, has been around for a while, but is really gathering momentum, and the issue of standardization is prevalent across the industry.

Patrick Grother is a computer scientist at NIST and has been involved in developing biometric specifications and evaluating algorithms for the institute.

"We do testing – typically of algorithms – and we are interested to know the core capabilities of algorithms on biometric data. We do it for face, for fingerprint, for iris and for speaker recognition," Grother said. "We do it for two reasons: One, we'd like to know the core capability of algorithms at processing data like that, and we publish this information because it's useful. The second reason is to give quantitative support to standardization."

When NIST is developing a new biometric specification, it typically sees participation from between ten and twenty vendors, Grother said. Tests can take months to a year and Grother often works in a small team of about five others.

NIST recently completed extensive tests on iris recognition, and found that it is a stable modality, which does not deteriorate over time. To

ards development in biometrics

Vrankulj

achieve this, Grother said finding a suitable dataset was a challenge, as it required long-term data.

"We were able to get log files from a frequent traveler system on the Canadian border with the U.S. and those logs come from a system that's been operating now for ten years," Grother said. "Those logs show – at their core – the similarity of a person's iris today, to their iris when they enrolled, up to ten years ago. In our view, operational datasets are the best way to look at the aging problem."

A particularly important standard for the law enforcement community is the American National Standard for Information System (ANSI). It refers to the standardized data format for the interchange of fingerprint, facial, scar mark and tattoo information.

According to the FBI's Brian Edgell, unit chief of the implementation and transition unit, Next-Generation Identification, the work that the FBI does would be impossible without the development of standards for biometric data.

"I can't overstate the importance of data exchanging," Edgell said. "Our foreign partners quickly get that when we sit down and they ask us about NGI or we talk about biometrics. They wonder: How can we bring 18,000 law enforcement agencies to the same system and exchange information as rapidly as we do, and as effectively and accurately as we do? Without standards, that would not happen. We would not have the ability to maintain the interoperable relationship with 50 states, dozens of federal agencies and the U.S. territories that we do without some sort of specifications."

The FBI works closely with NIST in developing the ANSI specification, which was first developed for the interchange of fingerprint information in 1993.

Besides the FBI, Interpol is another law enforcement body that relies heavily on standardized data.

"Interpol is precisely the kind of organization that benefits from having a standard," Grother said. "Their role in the criminal law enforcement community is predicated on the existence of standards. Data needs to come to them and

they need to be able to either search it themselves or use it themselves, or forward it to somebody else as a clearing house. It's perhaps the best example of interoperable biometric data."

Sebastien Taveau is a FIDO Alliance board member, an ex-pat from PayPal and is the current CTO at Validity Sensors – a company devoted to the consumer space.

"[In the government and law enforcement space] you are trying to match one vs. millions, which is fine, but consumers have little patience for that kind of matching," Taveau said. "You need to find a way to use the speed and convenience that consumers demand."

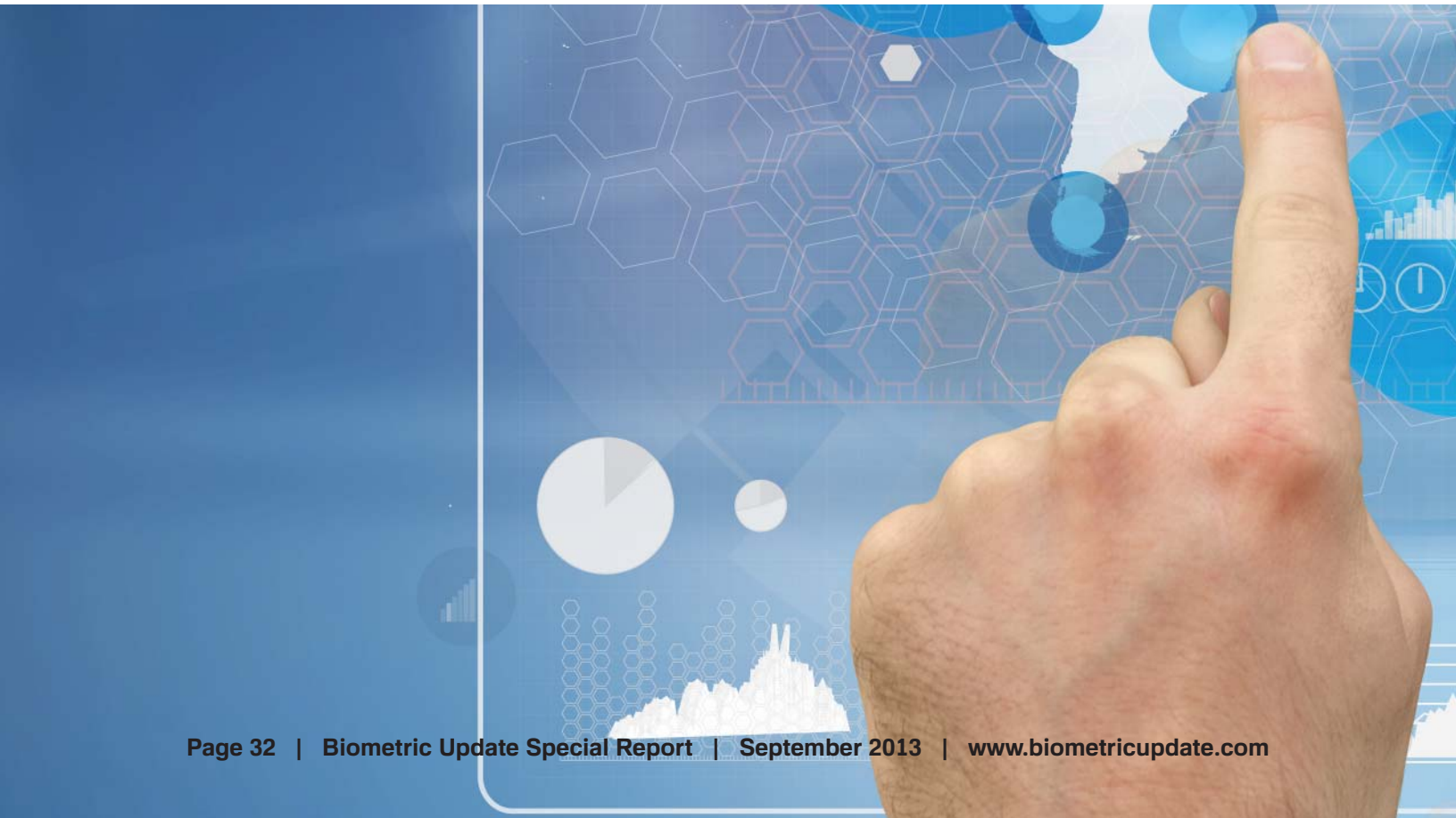
"You have to take a few steps back and look at the whole biometric ecosystem in and of itself. Until now, a lot of the standards that were developed were focused on what can be done with government-grade biometrics, and the restrictions that are put on those standards are different than what FIDO is trying to do."

The Fast Identity Alliance – FIDO for short – is a non-profit organization that was formed last year to address the lack of interoperability among strong authentication devices. The Alliance is developing specifications that aim to define an open set of mechanisms that goes beyond passwords to authenticate users online. Biometrics is a big part of this, and many companies have hopped on board to implement these open standards into their own offerings.

BlackBerry, CrucialTec, Google, Lenovo, Nok Nok Labs, NXP Semiconductors, PayPal, Validity, Yubico, Entersekt, EyeLock, Fingerprint Cards, FingerQ, Infineon, Ping Identity, Agnitio, Aktiv-Soft, Allweb Technologies, Arxan, Certus Technology Systems, Check-2Protect, Cloud Security, Crocus Technology, Diamond Fortress Technologies, Egis Technology, Facebanx, GoTrust Technology, Insyndia, It's Me!, LaunchKey, LG Electronics and SurePassID all count themselves members of this fast growing group.

Apple's launch of the iPhone 5S is a hot topic in the biometrics community, but Michael Barrett, president of the FIDO Alliance, thinks that without standards conformity, Apple's new device may not have the impact the community hopes it will.

"Apple's decision to include authen-



tication with the iPhone is a good dose of rocket fuel for the industry. Though any authentication technology unsupported by standards may take years, if ever, to achieve widespread market penetration," Barrett said. "The marketplace seeks authentication capabilities that span computer, smartphone, and physical access authentication and federated identity applications. Open industry standards, such as FIDO authentication specifications, are required before we can achieve industry-wide adoption of strong authentication across all platforms."

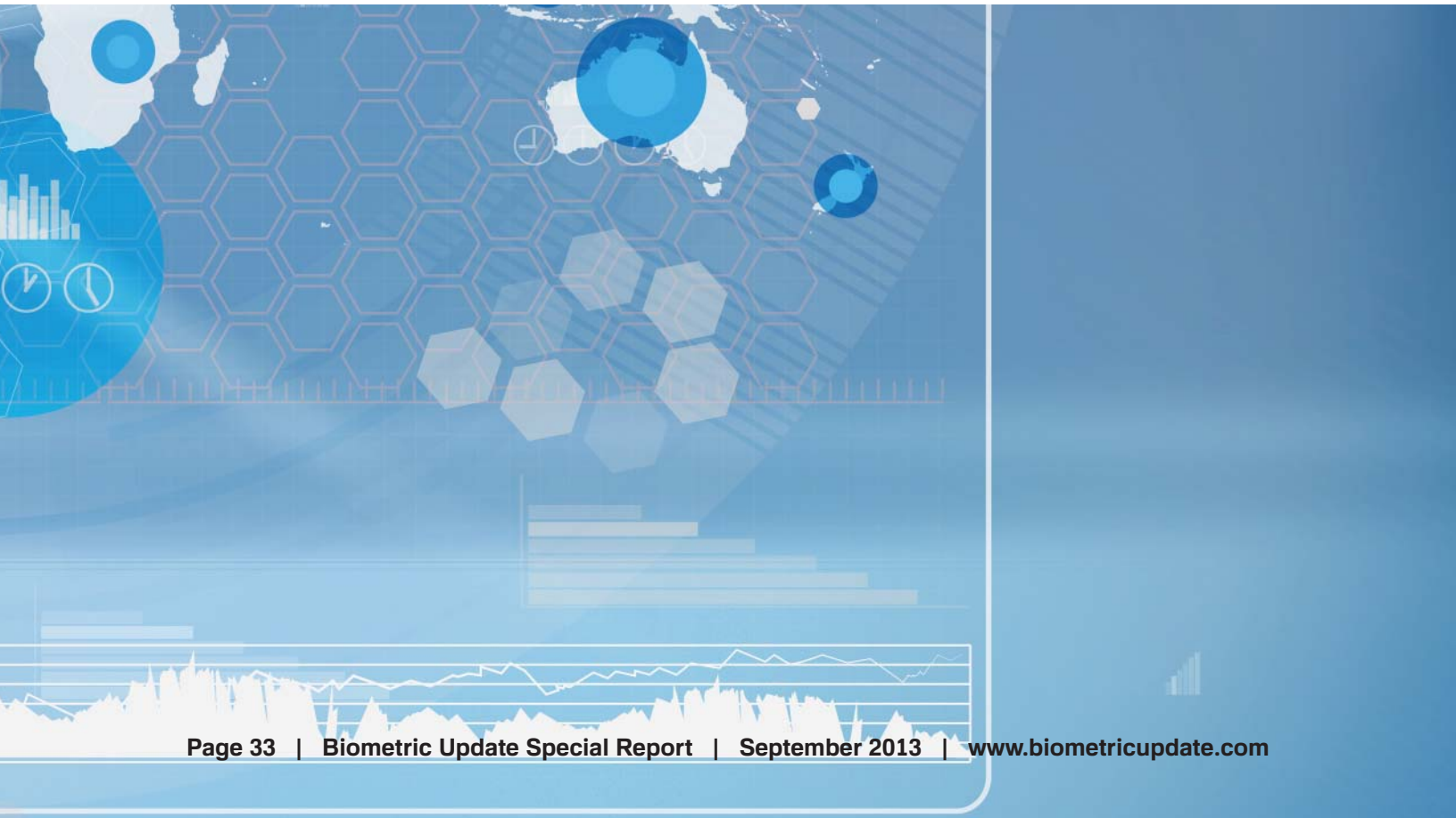
"It's estimated that Apple iOS penetration is only 17% of the total market, while PC and laptop fingerprint sensor penetration is at about 20% now, and has been thereabouts for years. Yet, though the PC market is provisioned, and now so is the Apple iPhone market, widespread penetration cannot and will not occur without open standards that make authentication methods interoperable. That's why the industry formed the FIDO Alliance, and that is how the industry as a whole will achieve widespread adoption of strong authentication."

According to Taveau, another consideration that must be made when creating standards is all of the other compliance certifications and standards already in place. For example, in the payment sphere, in which biometrics is quickly becoming a player.

"Some of our sensors are being used in industries that are new for any sensor provider, like payments. So now we have to look at designing hardware and software and make sure that these are integrated so they don't break the existing standards," Taveau said. "For example with EMV, which is for both payment cards and payment terminals. Let's say we add a fingerprint sensor to [that kind of system] -- that sensor cannot change the behavior of the terminal. If it does, the terminal manufacturer will lose its EMV certification."

Taveau said that standards are not only important on an industry-wide scale, but also internally for hardware development.

"When I joined Validity from PayPal, the first thing I did was I shipped all of our products to the best hackers in the world, in Berlin, and asked them to go after them like crazy. We learned a lot from that. That's why I say good luck if you're a bad guy, because the bad guys have already reviewed our products."



BiometricUpdate.com offers a directory of biometrics products and solutions providers. Find companies on this page to get more acquainted with organizations that can offer solutions to your biometrics needs and learn more about the dynamic businesses in this exciting industry.

Visit our website to submit your company to be listed in our biometrics directory.

Aware, Inc.
www.aware.com
40 Middlesex Turnpike
Bedford, MA 01730
USA

Since 1993, Aware has been a leading supplier of COTS biometrics software used in thousands of systems globally for government applications including border management, law enforcement, defense, credentialing, and access control.

BluStor PMC, Inc.
www.blustor.com
330 Gateway Place, Suite 500
San Jose CA 95110
USA

Protecting the full stream of mobile security.

Cognitec Systems GmbH
www.cognitec.com
Grossenhainer Str. 101, Tower B
01127 Dresden
Germany

Cognitec develops market-leading face recognition technologies and applications for enterprise and government customers around the world.

Cross Match Technologies, Inc.
www.crossmatch.com
3950 RCA Boulevard, Suite 5001
Palm Beach Gardens, FL 33410 USA

The worldwide standard in biometric identity solutions.

Warwick Warp
www.warwickwarp.com
The Venture Centre
Sir William Lyons Road
Coventry, CV4 7EZ
United Kingdom

Warwick Warp develops highly accurate fingerprint matching software. NIST verified, MINEX & STQC certified with development kits for AFIS, police and livescan applications.

Zwipe AS
www.zwipe.no
Gaustadalléen 21
Oslo Innovation Centre
0349 Oslo
Norway

Zwipe is the first contactless card with full on-card fingerprint scanning and matching functionality.

INDEX

COMPANIES

PEOPLE

ADVERTISERS

UPCOMING EVENTS

Homeland Security 2013
Oct 15-18, 2013
Washington, DC

Biometrics 2013
Oct 15-17, 2013
London, UK

Biometrics Institute Technology Showcase Australia
Nov 26, 2013
Canberra, Australia

2nd World BORDERPOL Congress
Dec 3-4, 2013
London, UK

Biometric Certification Training Boot Camp
Dec 9, 2013
Las Vegas, NV

STATS THAT DEFINE OUR INDUSTRY

U.S LAW ENFORCEMENT SPENDING

Bureau of Alcohol, Tobacco & Firearms

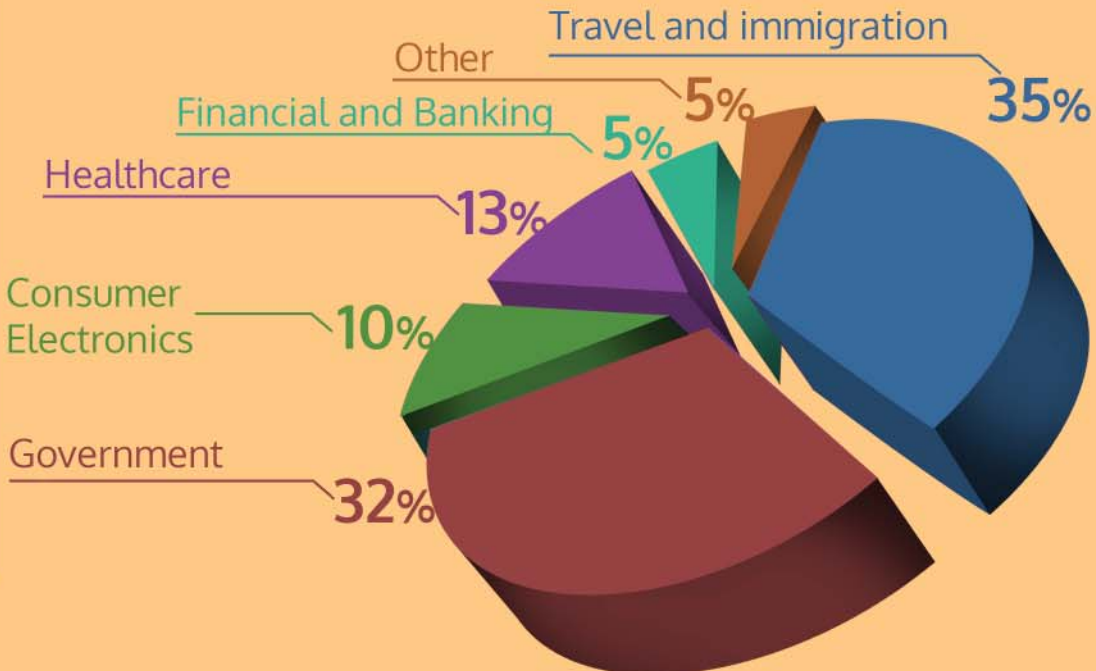
US Marshals Service

US Secret Service

Drug Enforcement Agency

Federal Bureau of Investigation

BIOMETRICS MARKET SHARE



Your company uses complex technology
to impact the human experience.

How well does your Web site
influence those same people?

If you believe your company Web site
could reach out to people more
effectively, contact us.

STUDIO1337

www.Studio1337.com 800.597.8712

Austin, TX Akron/Canton, OH Teesside, Durham Cty. UK