Law Enforcement and Biometrics

This white paper provides a brief, updated overview of the market size and technologies available for the law enforcement market in the United States.

Rawlson O'Neil King Lead Researcher, Biometrics Research Group.

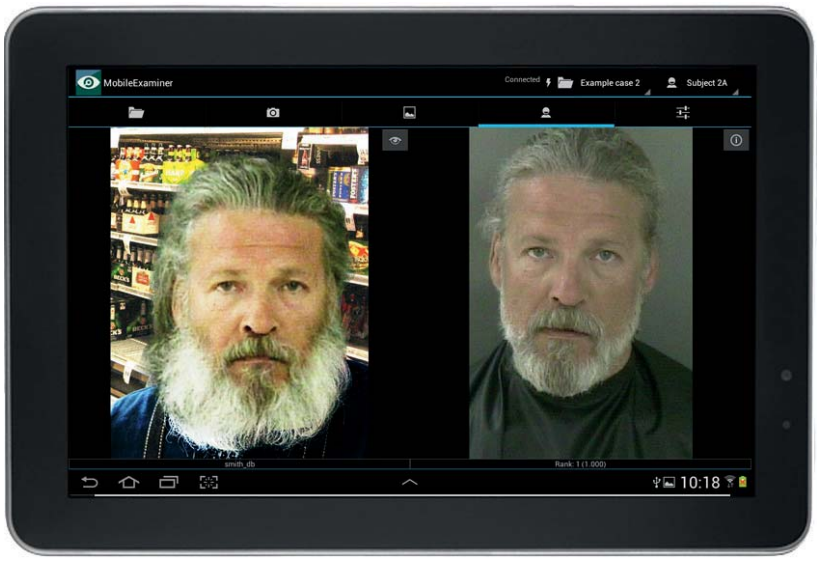
Premier face recognition technology

for fast and accurate criminal investigation

FaceVACS-DBScan with Examiner instantly matches crime scene photos, composites and surveillance video images against your mug shot repository to support efficient suspect identification.

The Examiner toolset enhances probe images to achieve faster and more accurate match results.

for image capture and search at the scene



FaceVACS-DBScan for Android devices allows agents to take suspect photos in the field, send authorized comparison requests to a centralized database and instantly receive a candidate list.

FaceVACS-DBScan runs as a stand-alone application or can easily integrate and interact with existing law enforcement IT environments.

Cognitec develops premier face recognition technologies and applications for facial image database search, video screening and analytics, border control, ICAO compliant photo capturing and facial image quality assessment.

About the Biometrics Research Group

Biometrics Research Group, Inc. provides proprietary research, consumer and business data, custom consulting, and industry intelligence to help companies make informed business decisions.

We provide news, research and analysis to companies ranging from Fortune 500 to small start-ups through market reports, primary studies, consumer research, custom research, consultation, workshops, executive conferences and our free daily BiometricUpdate.com news service.

Biometrics Research Group has positioned itself as the world's preferred supplier of pure-play market research and consultancy services focused on the biometric marketplace, which particular focus on the law enforcement and national security sectors. Our portfolio of white papers and full research reports is based upon high-quality quantitative analysis, allowing our clients to gain deeper understanding of the marketplace.

We customize our research design, data collection, and statistical reporting using proprietary micro- and macroeconomic modeling and regression analysis.

Through integration of our research results with qualitative analysis from our BiometricUpdate.com news service, we provide actionable business analysis.

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.

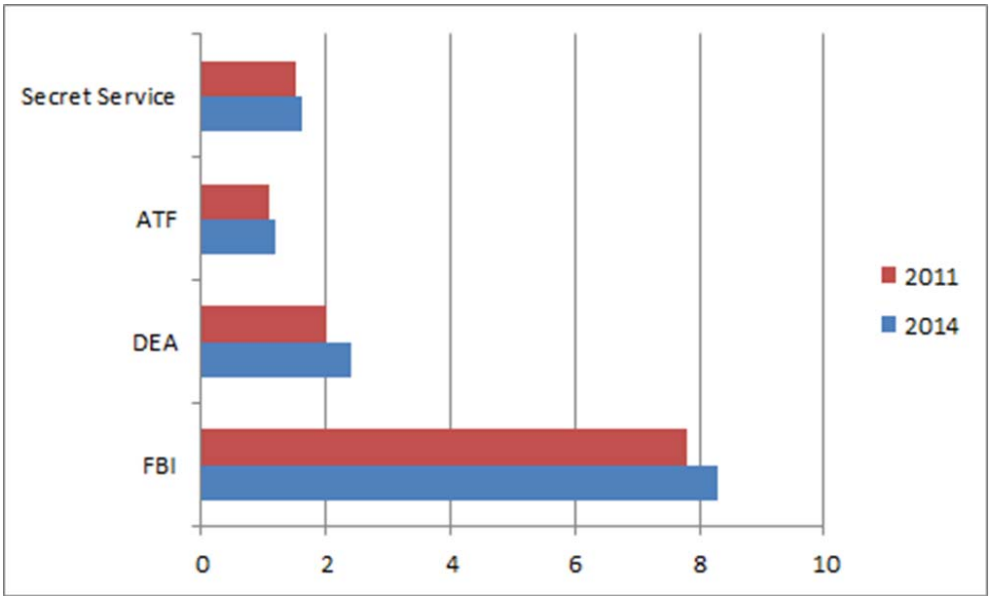
Biometrics Research Group, Inc. defines biometrics as a physical trait or pattern which is unique to every individual. It is often used to verify and authenticate a person's identity that is enrolled into a system. Biometric patterns can be anything from fingerprints, iris scans, facial recognition or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

The law enforcement market is characterized by the widespread use of biometric technologies, automated fingerprint identification technology, voice, iris, and facial recognition, implemented at the state and federal levels across the United States and around the world. Increasingly, DNA is being used by criminal justice agencies as well.

Market Size

Measuring the resources expended by the U.S. federal government for law enforcement is not a simple process. Funding is appropriated and expended by multiple organizations and the activities for which it is spent may include non-law enforcement activities. For example, the U.S. Coast Guard has a wide range of security, safety and law enforcement functions that often blend together and overlap, making a direct accounting of law enforcement spending difficult. As a result, our calculations will only incorporate the budgets of the FBI, DEA, ATF and the Secret Service.

U.S. Law Enforcement Spending in Billions (2011 & 2014)



In the 2014 fiscal year, the U.S. government budgeted US$8.3 billion for the FBI, which was US$232 million above the fiscal year 2013 enacted level. The U.S. Drug Enforcement Agency (DEA) was funded at US$2.4 billion in 2014, an increase of US$21 million above the fiscal year 2013 enacted level. The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) was funded at US$1.18 billion, US$47 million above the fiscal year 2013 enacted level. The U.S. Secret Service budgeted US$1.6 billion, a decrease of US$27 million below the fiscal year 2013, due to savings from reduced operations after the presidential election cycle.

Police spending mostly takes place at the state and local levels, which further complicates accounting. Local law enforcement spending however is estimated at US$68.6 billion in the states and US$161.6 billion by local governments, respectively in fiscal 2014.

In fiscal year 2012, the U.S. Government spent US$14.4 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. Local U.S. governments spent approximately US$100 billion generally on total police services in fiscal year 2012.

In fiscal year 2011, the budgets of the FBI, DEA, ATF and the Secret Service totaled US$12.5 billion.

Resources of Major Federal Law Enforcement Organizations (FY2011)

Department	Agency	Budget ($ Millions)	Staff Level
Justice	Federal Bureau of Investigation (FBI)	7,849	32,998
	Bureau of Alcohol, Tobacco, and Firearms (ATF)	1,121	5,101
	Drug Enforcement Administration (DEA)	2,020	8,399
	Bureau of Prisons (BoP)	6,185	40,563
	U.S. Marshals Service	1,152	5,544
	U.S. Attorney's Office	1,934	10,629
Homeland Security	Customs and Border Protection (CBP)	9,880	59,820
	Immigration and Customs Enforcement (ICE)	5,501	20,546
	U.S. Coast Guard (USCG)	8,593	50,682
	U.S. Secret Service (USSS)	1,515	7,054

Sources: FY 2011 budget summaries of the Federal Bureau of Investigation; Bureau of Alcohol, Tobacco and Firearms; Drug Enforcement Agency; Bureau of Prisons; United States Marshals Service; Customs and Border Patrol; Immigration and Customs Enforcement; United States Coast Guard; and United States Secret Service.

Other agencies such as the Bureau of Prisons, U.S. Marshals Service, U.S. Attorney's Office, Customs and Border Protection, Immigration and Customs Enforcement and the Coast Guard, were excluded from this analysis, since their missions are not solely within the realm of law enforcement.

Distribution of Law Enforcement Officers across Organizations (2012)

Department	Component Office	Correctional Officers	Park Ranger	U.S. Marshal	Police	Inspection	Investigation	Customs and Border Patrol	Aircraft Operations	Total
Homeland Security	Customs and Border Protection					700		43,154	1	43,855
	Immigration and Customs Enforcement					6,047	6,863			12,910
	Other Offices				121	88	533			742
	United States Secret Service				944	167	3,015			4,126
	Department Total				1,065	7,002	10,411	43,154	1	61,633
Justice	Bureau of Alcohol, Firearms, and Tobacco					27	2,463			2,490
	Bureau of Prisons	19,125								19,125
	Drug Enforcement Administration					1	4,774			4,775
	Federal Bureau of Investigation				230		13,637			13,867
	Other Offices						150			150
	United States Marshals Service			803		127	3,132		1	4,063
	Department Total	19,125		803	230	155	24,156		1	44,470
Interior	Department Total	178	1,531		868	210	546		4	3,337
Treasury	Department Total				499	2	3,010			3,511
Defense	Department Total	8			7,779	4	2,047		1	9,839

Source: Data received from Office of Personnel Management on March 12, 2012.

Biometrics Research Group calculates that most of the cost of law enforcement activities within these organizations is allocated for labor.

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.

A M2SYS white paper noted the most common biometric modalities used in law enforcement include:

Fingerprints: Fingerprint recognition has been the standard biometric modality for law enforcement agencies for a long time and still is.

Palm Print Biometrics: Legal systems and law enforcement agencies in the United States have increasingly used using palm print authentication for prisoner identification, crime scene investigation and prison management for couple of years, as about 30 percent of all the latent found at a crime scene are palm prints.

Facial Recognition: Facial recognition is a relatively new biometric modality which is recently gaining the attention of law enforcement agencies. It can be useful as a surveillance tool for law enforcement agencies by reducing the number of possible matches in a data pool to a manageable amount.

Iris Recognition: Iris recognition is another biometric modality of recent interest for law enforcement. Until now, iris recognition has been used in some places in a commercial capacity for verification but law enforcement agencies are starting to use it more frequently as a way of looking for more sophisticated and accurate authentication systems of identification.

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. ***In 2015, Biometrics Research Group estimates that spending on fingerprint systems totalled US$5 billion, while spending on the other combined biometric modalities equalled US$2.5 billion. Biometrics Research Group projects that total spending on biometrics for law enforcement increased to US$7.5 billion in 2015.***

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.

10 YEARS OF ADVANCING IDENTITY TECHNOLOGY...

NEW FOR 2016:
- Maryland Test Facility (MdTF) Site Tour
- NIEM Biometrics Training

BIOMETRICS FOR GOVERNMENT & LAW ENFORCEMENT

January 25th-27th, 2016 • Washington, DC

Identity Innovation: Requirements for Advanced Recognition, Processing, and Analytics for Government and Law Enforcement Applications

Featured Speakers

Amy Hess
Executive Assistant Director
FBI (Science and Technology Branch)

Kenneth D. Gantt
Deputy Director
Office of Biometric Identity Management (OBIM)
DHS

Wolf Tombe
Chief Technology Officer
U.S. Customs and Border Protection

Nick Megna
Unit Chief BCOE
FBI CJIS Division

Identity Innovation Workshops Featuring NIEM and ARL

Dr. Suowen Hu
Army Research Labs

Will Graves
DoD Biometrics
Deputy Product Manager/ Chief Engineer

Kamran Atri
CSE CTO
NIEM Expert

Ten Featured Topics for the 10th Annual Event

- NIEM Biometrics Training Workshop
- DHS Maryland Test Facility (MdTF) Site Tour
- Video and Voice Analytics
- Data Filtering for Interoperable Systems
- Homeland Advanced Recognition Technology
- Rapid DNA
- Facial Recognition Modality at the Border
- Multimodal Biometric Authentication
- Systems Interoperability
- Mobile Biometrics Technology

Sponsors: integenX® NORTHROP GRUMMAN 3M Science. Applied to Life.™

Register Today! www.BiometricsEvent.com • 1-800-882-8684 • idga@idga.org

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 estimates that U.S. Government spending has been stable since 2013 at a rate of at least US$700 million per annum on basic biometric research.

A further key development which is impacting biometrics in law enforcement is the advent of cloud biometrics. According to a M2SYS white paper, the implementation of cloud-based solutions, in conjunction with mobile devices, has become an increasingly popular option.

The firm notes: "Cloud-based mobile and biometrics enabled solutions can aid law enforcement officials around the globe to identify wanted criminals by comparing their biometric data against a wide variety of offender databases on the go. Mobile and cloud based biometric identity verification can prevent unnecessary trips back to the station or unwarranted arrests. These solutions don't only safeguard the public against identity fraud but also save police department manpower allowing for more comprehensive and accurate coverage and an increase in public safety."

Biometrics Research Group, Inc. estimates that cloud-based solutions will constitute at a minimum 50 percent of biometric offerings marketed to law enforcement agencies in the United States by 2020. In terms of revenue breakdown, we estimate that cloud-based solutions will total US$12.5 billion by 2020.

Next Generation Biometric System

In 2013, Biometrics Research Group, Inc. projected 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. In 2014, the FBI announced it had digitally converted millions of files stored at its Criminal Justice Information Services (CJIS) division, in an effort to transition to its new so-called "Next Generation" biometric system.

Over the last two decades, the agency has digitally converted more than 30 million records including criminal history folders and civil identity, and as many as 83 million fingerprint cards. This resulted in the dismantling of thousands of filing cabinets once hand-searched by Bureau staff.

The massive conversion was part of a FBI initiative to prepare for the activation of Next Generation Identification (NGI) system, an advanced digital platform of biometric and other types of identity information. Incrementally replacing the FBI's Integrated Automated Fingerprint Identification System (IAFIS), the new system, which cost US$1.1 billion to implement, is designed to better serve its high-profile users, including law enforcement agencies checking criminal histories and fingerprints, veterans, government employees, and the FBI's own laboratory.

In 1999, the FBI implemented the NGI 10-year contract to replace its previous 15-year-old Integrated Automated Fingerprint Identification System (IAFIS) with an advanced biometrics system, adding several new capabilities for federal and local law enforcement officials to more effectively identify suspects.

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 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) held all fingerprint sets collected in the United States, and was managed by the FBI. Launched in 1999, the FBI's database was 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 was 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 has lead innovation in the AFIS field by adding 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 announced its decision to widen its Integrated Automated Fingerprint Identification System (IAFIS) to become multi-modal. As part of its Next Generation 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 cur-

rent 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 is 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 expanding 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.

In addition to being used by the FBI and local police forces, the NGI now is used regularly by the U.S. Department of Homeland Security as the agency sends prints to NGI from all border crossings and port of entry checkpoints. Additionally, the Defense Department and the Office of Personnel Management regularly depend on the FBI to process fingerprints against NGI.

DNA

Law enforcement is coming to increasingly rely on the use of DNA-based technologies as an aid in solving crimes. Although not yet at the point of other biometric technologies in terms of speed, DNA matching cannot be ignored in this discussion. DNA is being used to process criminal suspects to separate the guilty from the innocent. It is also being used to identify victims and to match convicted offenders to outstanding crimes. To aid these processes, the establishment of DNA data banks is either underway or under consideration in several jurisdictions including Canada and the United States.

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 antiparallel strands that spiral around each other in the form of a double helix.

DNA is an excellent biometric identifier because it is 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.

The acronym CODIS describes not only the software used to maintain and operate law enforcement DNA databases but also the FBI's program of software support and training for federal, state, local, and international forensic laboratories. The acronym NDIS stands for the National DNA Index System or National DNA database, the highest level of the CODIS hierarchy (national, state, and local).

One of the underlying concepts behind the development of CODIS was to create a database of a state's convicted offender profiles and use it to identify suspects for crimes in which there are no suspects. Historically, forensic examinations were performed by laboratories if evidence was available and there was a suspect in the case. Beginning in the early 1990s, states began to create databases of the DNA profiles of convicted sex offenders and other violent criminals. The databases allowed federal laboratories to analyze those cases without suspects and search those DNA profiles against the database of convicted offenders and other crime scenes and determine if a serial or recidivist rapist was involved. It is expected that this new tool will enable forensic laboratories to generate investigative leads or identify suspects in cases, such as stranger sexual assaults, where there may not be any suspects.

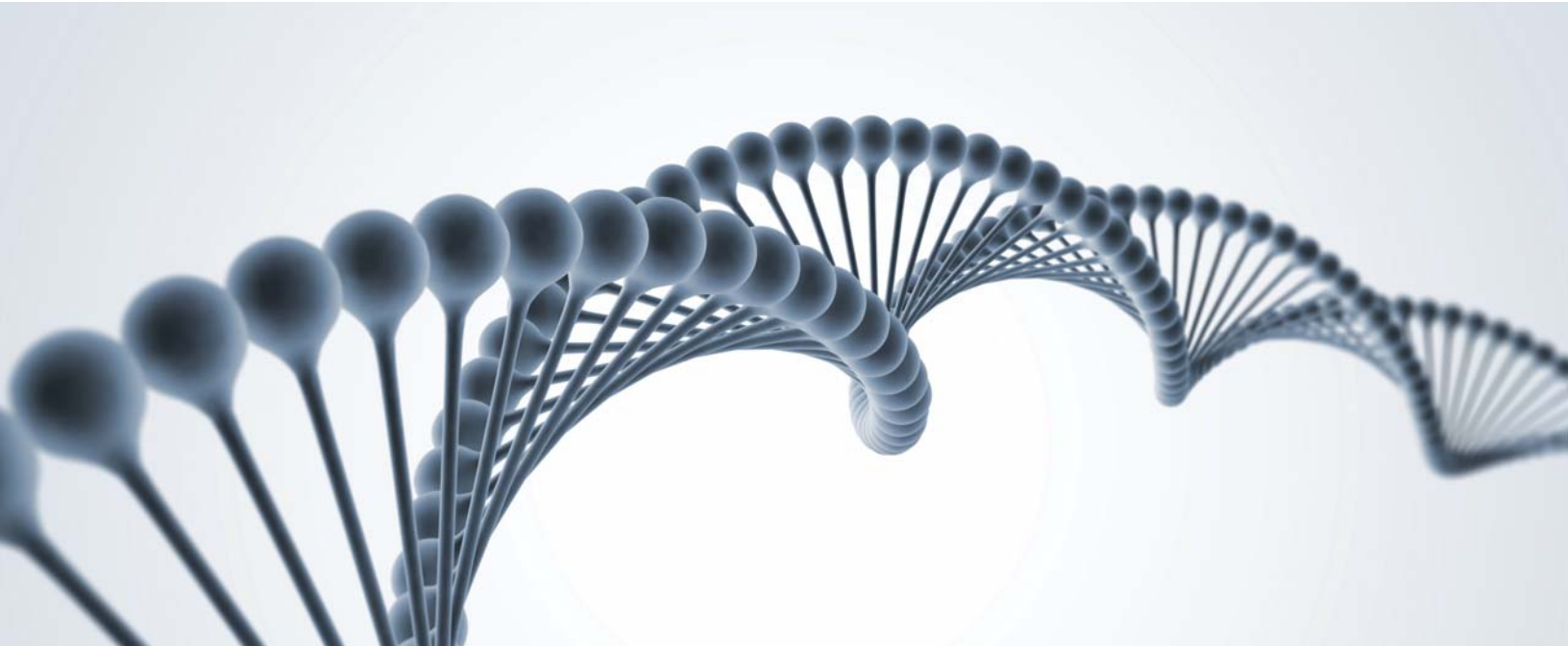
An identification tool that was initially thought to benefit the investigation of sexual assault cases has proven to have wider application in the investigation and prosecution of crimes. States have observed this firsthand with their CODIS hits and sought to expand coverage of their databases beyond convicted sexual offenders—first to more serious violent felony offenders, then all felony offenders, and now to persons arrested for sexual offenses and, in many states, persons arrested for any felony offense. Currently, 26 states, the federal government, the Department of Defense, and Puerto Rico upload DNA profiles of various categories of arrestees to NDIS. Twelve states are collecting DNA samples from all felony arrestees, and another 15 states are authorized to collect DNA samples from persons arrested for serious felonies such as murder, manslaughter, kidnapping, sexual assault, robbery, and burglary. Another dozen states have legislation pending to authorize the collection of DNA samples from arrestees or to expand their current coverage of arrestee sample collections.

The CODIS software is used to maintain these DNA databases and search the DNA profile against the DNA profiles of convicted offenders/arrestees and other crime scenes. For example, a DNA profile of a suspected perpetrator is developed from the sexual assault evidence kit. If there is no suspect in the case or if the suspect's DNA profile does not match that of the evidence, the laboratory will search the DNA profile against the Convicted Offender and Arrestee Indices. If there is a match in the Convicted Offender or Arrestee Index, the laboratory will obtain the identity of the suspected perpetrator. If there is no match in the Convicted Offender or Arrestee Index, the DNA profile is searched against the crime scene DNA profiles contained in the Forensic Index. If there is a match in the Forensic Index, the laboratory has potentially linked two or more crimes together and the law enforcement agencies involved in the cases are able to share the information obtained on each of the cases.

The FBI Laboratory works closely with the DNA and CODIS communities as well as other stakeholders, such as laboratory accrediting bodies, law enforcement, defense attorneys, and prosecutors, to evaluate new technologies and procedures for the CODIS program (e.g., familial searching, NDIS enhancements, Rapid DNA). Over the years, the CODIS software has been updated to include the collection and maintenance of additional data elements to facilitate missing person searches, upgraded telecommunications circuits, and routers, to name a few. Many of these CODIS technologies and procedures included consultation with the affected stakeholders, software development, testing, evaluation, implementation planning, and user training; processes that the FBI continues to follow for Rapid DNA.

CODIS is installed in approximately 200 federal, state, and local forensic DNA laboratories nationwide. The FBI provides the CODIS software to public forensic DNA laboratories that are accredited, that follow the FBI Director's quality assurance standards, that are audited annually, and that agree to comply with the Federal DNA Act for participation in NDIS. To date, CODIS has generated more than 285,000 investigative leads for law enforcement. All 50 states, the FBI, the U.S. Army Criminal Investigation Laboratory, and Puerto Rico contribute DNA records to and participate in the National DNA Index System. As of June 1, 2015, NDIS contains almost 14 million offender/arrestee DNA records and over 630,000 forensic (crime scene) DNA records.

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.



MORPHOBIS IN THE CLOUD

MORPHO CLOUD RAISES BIOMETRIC IDENTIFICATION TO NEW HEIGHTS

CRIME SOLVING CAPABILITY – *EMPOWERED*

SYSTEM AVAILABILITY – *UNLEASHED*

DATA SECURITY – *ASSURED*

COLLABORATION POTENTIAL – *UNLIMITED*

AFIS AS A SERVICE

Morpho Cloud is a secure and flexible AFIS as a Service solution for Morpho's flagship Biometric Identification Solution (MorphoBIS). Morpho Cloud is hosted on Microsoft Azure Government, the cloud platform designed to meet the U.S. government's requirements for data security and continuity of operations. Backed by the Microsoft Azure Government platform, Morpho Cloud complies with the stringent security standards for storage, transmission, monitoring, and recovery of digital information, including standards issued by the FBI's Criminal Justice Information Services (CJIS).

FLEXIBLE IMPLEMENTATION

Morpho Cloud offers several configuration options addressing your agency's specific operational requirements:

- Disaster Recovery with system replication in the Cloud
- Tailored AFIS with a full Cloud solution
- Standard AFIS with a full Cloud solution

MorphoTrak
Contact Us: 1-800-368-9505 • www.morpho.com/USA
5515 E. La Palma Ave. Ste. 100
Anaheim, CA 92807

SAFRAN
Morpho

Rapid DNA

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.

Field-testing has also occurred of another mobile, Rapid DNA lab service that yielded full DNA profiles 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.

It is important to note that Rapid DNA is still considered experimental. The FBI uses the term "Rapid DNA analysis/technology" to describe the fully automated (hands-free) process of developing a CODIS Core Short Tandem Repeat (STR) profile from a reference sample buccal swab. The 'swab in—profile out' process consists of automated extraction, amplification, separation, detection, and allele calling without human intervention. The FBI's objective for Rapid DNA technology is to generate a CODIS-compatible DNA profile and to search these arrestee DNA profiles within two hours against unsolved crime (forensic) DNA while an arrestee is in police custody. Rapid DNA technology has been designed for use within and outside the forensic DNA laboratory, as the Rapid DNA instruments are self-contained machines that require no human intervention beyond the loading of the DNA samples and analysis cartridges into the machines.

Following any legislative authority, the FBI envisions Rapid DNA integration occurring in two-phases. Phase 1 involves the booking station CODIS enrollment and searching of Rapid DNA profiles. Phase 2 of integration is the direct "hit notification" to booking stations and investigative agencies. The initial (Phase 1) impact of Rapid DNA analysis in the booking station will be the elimination of the weeks-to-months it currently takes for arrestee samples to be mailed, received, inventoried, and analyzed for registration in the CODIS system. The eventual real time notification (Phase 2) of an arrestee's DNA hit to an unsolved case is expected to conserve valuable investigative resources and focus them on specific arrestees. Equally as important will be the protection of the public when perpetrators are identified at the point of collection before being released back into their communities at the completion of the normal booking process. Rapid DNA CODIS registration will not lengthen the booking process.

The FBI initially established a Rapid DNA initiative in 2006 and partnered in 2008 with the Departments of Defense and Homeland Security on the development of point-of-collection DNA analysis for the production of CODIS DNA profiles (containing the 13 CODIS Core Loci) within a two-hour period. In 2010, the Criminal Justice Information Services' Advisory Policy Board (CJIS APB, a federal advisory committee established by the FBI) established a Rapid DNA Task Force, and the FBI's Rapid DNA Program Office was created within the FBI Laboratory Division to coordinate the Laboratory and CJIS Division's Rapid DNA activities. These groups have provided the FBI with recommendations that it has adopted for its Rapid DNA implementation, such as the use of the State Identification Number (SID) as the cornerstone identifier for Rapid DNA profiles and the addition of a data element to an individual's criminal history record to indicate whether there is a DNA profile already in CODIS, information which will assist states in determining if a DNA sample should be collected at arrest.

For implementation within an accredited forensic laboratory, the Scientific Working Group on DNA Analysis Methods (SWGDAM) empanelled a Rapid DNA Committee to review and evaluate whether additional quality measures were necessary to ensure the accuracy and reproducibility of the records produced by the Rapid DNA instruments. Based upon recommendations received from SWGDAM, the FBI issued an addendum to the quality assurance standards for DNA Databasing Laboratories, required by Federal law, providing a foundation for implementation of Rapid DNA within an accredited forensic DNA laboratory.

The FBI Laboratory is also developing CODIS software modifications to facilitate the searching of Rapid DNA instrument-generated DNA profiles against forensic DNA records. Along with these development efforts, steps are being taken to identify information technology enhancements needed for state criminal history record repositories, booking stations, regional, county, and local jails, to comply with FBI CODIS requirements for uploading DNA records generated at the time of arrest. As noted previously, Rapid DNA technology has been designed for both laboratories (approximately 200 forensic DNA laboratories participating in CODIS) as well as law enforcement booking agencies across the nation (potentially thousands of law enforcement booking facilities).

The CJIS and Laboratory Divisions are working together to determine the interfaces necessary for the integration of the Rapid DNA components into the criminal history record and booking station infrastructure originally established for the Automated Fingerprint Identification System (AFIS). As one example, integration of the Rapid DNA instruments with CODIS and Arrestee State Identification Numbers is necessary to facilitate the notification of CODIS hits to law enforcement agencies in order to act on investigative leads. The FBI Laboratory's Rapid DNA Program Office is working with the CJIS APB's Rapid DNA Task Force to plan Rapid DNA workflows and develop requirements for implementation.

The Federal DNA Act requires that the DNA records maintained at NDIS be generated by accredited laboratories in compliance with the FBI Director's quality assurance standards (42 U.S.C. §14132(b)). Rapid DNA technology has been designed for use by law enforcement agencies at the point of booking for integration following live scan fingerprint enrollment of an arrestee. Thus, statutory authorization for the use of FBI approved Rapid DNA instruments by criminal justice agencies would be needed before the DNA records generated at police booking stations can be searched at NDIS.

Conclusion

Biometrics Research Group, Inc. notes that the market size for biometric applications in the law enforcement segment continues to grow. 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.

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 US$1 billion, totalling US$4 billion in overall spending. Biometrics Research Group, Inc. projects that total spending on biometrics for law enforcement increased to US$7.5 billion in 2015. In 2015, Biometrics Research Group estimates that spending on fingerprint systems totalled US$5 billion, while spending on the other combined biometric modalities equalled US$2.5 billion. While fingerprint matching, palm print biometrics, facial and iris recognition are considered growth areas, we project that DNA will play an increasingly important role as an emerging biometric modality used with greater regularity by law enforcement agencies in the United States.

---

1. Steven Payson, Public Economics in the United States: How the Federal Government Analyzes and Influences the Economy: How the Federal Government Analyzes and Influences the Economy. (ABC-CLIO: 2014).

2. Tanvir Ahmed, “Cloud-Based Biometrics Will Change the Face of Law Enforcement”, M2SYS Blog On Biometric Technology (blog), March 24, 2015, accessed November 18, 2015, http://blog.m2sys.com/public-safety/cloud-based-biometrics-will-change-the-face-of-law-enforcement