Almost a decade has passed since one of the most sensational criminal cases in American history turned a suspicious eye inward toward the American criminal justice system. More specifically, that suspicious eye turned toward law enforcement officers and their professional conduct surrounding the collection, preservation, storage, and custodial chain of evidence. Most notably and arguably, the evidence trail has become perhaps more important than the actual evidence collected during a criminal investigation. Furthermore, the volatile nature of digital evidence and the exponentially increasing occurrences of crimes, directly or indirectly, involving computer technologies and digital evidence, compels the investigation, contemplation, and implementation of innovative, technological approaches to preserve evidentiary value and raise the bar for collecting and tracking physical and digital evidence.

It is our position that the sophistication and consistent advancements of biometric technologies could provide substantial benefits within the criminal justice system, assist in mitigating erroneous law enforcement procedures and processes prone to human error, and enhance the integrity of physical and digital evidentiary value. The application of biometric technologies within law enforcement environments is boundless. The integrity of this environment rests on the crisp and accurate answer to the simple question: who did what when?

The advancement of new biometric technologies that combine portability, trustworthiness, afford privacy and are cost-effective make the broad deployment of biometric devices possible. The criminal justice system currently deploys successful biometric systems inside a small number of correctional facilities, and obviously, the standard utilization of the automated fingerprint identification system (AFIS) suggests that the criminal justice system is embracing new biometric technologies, however modernization within this system is often laggard. In a paper published by The Futures Working Group (FWG), entitled Improving Our View of the World: Police and Augmented Reality Technology, the authors state the following corroborating statements:

“The professions’ [law enforcement] customary luxury of playing ‘catch-up’ to technological advances is no longer a viable option. The accelerated speed of change in the information age requires police agencies to adopt a new approach and redefine missions in new, strategic terms... Indeed, while much of the rest of the world entered the digital age in the 1990’s, and radically altered its business processes and methodologies to take advantage of new technology, many police departments have changed very little... The crucial component to effective policing in a rapidly changing world is this ability to think creatively about emerging technologies and how they can be used successfully within the constitutional limitations of a free society. Many new devices give us the ability to do what has always been done better or faster or more efficiently than in the past.”

We believe the successful implementation and application of biometric technologies can support the law enforcement officer, often overwhelmed with paperwork and paper trails, to assure that evidentiary value remains intact, organizational processes and procedures are improved, and ameliorate security requisitions, beginning with the initial collection of evidence throughout the presentation of evidence in court, especially considering the critical assessments and tactics deployed by the notorious defense lawyer to identify weaknesses in law enforcement methods. It is our position that the use of biometric technologies in the criminal justice system is not only feasible, but will be definitive in transposing current, manually intensive responsibilities inherent to the criminal investigation.

Although a comprehensive and detailed explanation of biometric technologies is beyond the scope of this paper, we will take a brief look at the introduction of the fingerprint into the criminal justice system, provide brief—although fundamental—concepts of biometric methodologies and subsequent techniques, introduce opportunities for integration within the criminal justice system, and finally, state some advantages and disadvantages to the use of biometrics.

---

The foundation of modern biometrics spans three thousand years of development. The methodologies used to establish an individual’s identification based upon distinguishable, unique, physical characteristics can be dated back to 1000 BCE with archaeological evidence from ancient civilizations. Evidence suggests fingerprints were used as a legally binding signature in ancient Chinese societies, the Babylonians used fingerprints in business transactions, and 14th century Persian government documents included fingerprint impressions. A professor of anatomy observed the ridges, spirals, and loops in fingerprints in 1686, while another professor of anatomy published his hypothesis categorizing nine different fingerprint patterns in 1823; neither professor identified the intrinsic value of the fingerprint for identification. In 1856, Sir William Hershel, an English magistrate, required the additional impression of a fingerprint on contracts to deter attempts of repudiating a written signature; he is historically the first individual to note the unique characteristics and permanence of the fingerprint. Within the next fifty years, the use of fingerprints as identifying credentials would be gently maneuvered into law enforcement and correctional environments.

Dr. Henry Faulds is credited as the first individual to recognize the significance of the fingerprint to identify one individual from another. In 1880, he developed a fingerprint classification system and a recording method for identification purposes. He subsequently attempted to recruit the assistance of Sir Charles Darwin, the renowned naturalist for his theories of evolitional development. Due to poor health (Darwin died in 1882), Darwin forwarded Faulds’ materials to his cousin, Sir Francis Galton. Galton’s interests, observations, and published articles presented the fundamental foundations of modern fingerprinting systems to the masses. In an article published in 1888, Galton describes the fingerprint as, “[p]erhaps the most beautiful and characteristic of all superficial marks… [t]hese lines are found to take their origin from various centers… [t]hey proceed from their

4 Ibid.
5 Ibid.
6 http://www.jaypeetex.com/products/Law%20Enforcement/AFIS/Palm.htm
several centers in spirals and whorls, and distribute themselves in beautiful patterns over the whole palmar surface. Finally, in 1901, Sir Edward Richard Henry revised Galton’s observations and theories thereby establishing the Henry Classification System in England; this is the system used by law enforcement today.

With the advent of the Henry Classification System, the discipline of biometrics as a means of identification was successfully embraced by the criminal justice system. Modern biometric implementations within the criminal justice system have evolved from the laborious, manual, expert examination of two separate fingerprints for correlating minutiae points to the adoption of sophisticated and advanced technologies. With the progression of sophisticated computer technologies, the science of biometrics is comprised of not only fingerprints, but also a number of other physical and behavioral characteristics that successfully differentiate one individual from another.

Biometric technologies specialize in comparing unique physical or behavioral human characteristics. A physical biometric characteristic must be universal to all, remain primarily consistent throughout a lifetime, be unique to each individual, and be resistant to manipulation or destruction. Currently, the most widely recognized, respected, and deployed biometric technology is the fingerprint device. Algorithms convert key reference points, or minutiae points, from a digitally scanned image of a fingerprint into a mathematically based template, and the template can then be stored on various storage media. Other physical biometrics technologies include facial recognition, hand geometry, iris scan, retinal scan, and vascular patterns.

Physical biometric technologies are considered more reliable than behavioral biometric characteristics. Alternatively, behavioral biometric technologies collect, store, measure and compare learned behaviors of an individual. The premise is that an individual cannot easily manipulate an acquired, learned behavior. For example, behavioral biometric technologies can analyze voice patterns, analyze signature forces and motions, or analyze keystroke methods specific to an individual. Obviously, behavioral biometric technologies are less reliable than their physical counterparts. Table 1 below briefly outlines physical and behavioral device methodologies.

---

<table>
<thead>
<tr>
<th>Physical Characteristics</th>
<th>Behavioral Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device</strong></td>
<td><strong>Methodology</strong></td>
</tr>
<tr>
<td>Fingerprints</td>
<td>Extracts distinct characteristics called minutiae from live scanned fingerprint; converts minutiae into a digital comprised template for storage; identification and verification are based upon statistical values of correlating minutiae. Device technologies include optical readers, silicon chips, ultrasound and tactile sense.</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>Exterior geometry uses dimensions and distances between features on the exterior of the hand to create and match templates. Interior scanning creates an image of the user’s hand using infrared light and then identifies individual patterns based on blood vessels and connective tissue.</td>
</tr>
<tr>
<td>Iris Scanning</td>
<td>Based on the individual characteristics of the iris, which include features such as rings, furrows, and freckles to form the biometric “iris code”.</td>
</tr>
<tr>
<td>Retina Scanning</td>
<td>Recognition uses the individual pattern of blood vessels apparent on the surface of the retina to create templates and assess matches; retinal template has more individual feature-points than any other biometric in current use.</td>
</tr>
<tr>
<td>Facial Recognition</td>
<td>Identifies distinct features of a user’s face, measures distances between features of the face, and stores a digital representation of this template. Verification and identification is based upon statistical analysis of a live scanned image and a stored template.</td>
</tr>
</tbody>
</table>
Another fundamental concept of biometrics includes differentiating between the two primary purposes of any biometric technology. Biometric technologies provide two distinct underlying operatives, identification and verification (a.k.a. authentication). Identification occurs when an individual’s live, scanned fingerprint image is matched against all the fingerprint templates stored in a database (i.e. Automated Fingerprint Identification System - AFIS). Identification is a one-to-many comparison. Alternatively, verification is a one-to-one comparison. In the verification operative, in essence, an individual states, “this is who I claim to be and this is my fingerprint template”. The biometric technology compares the live, scanned fingerprint template against one previously stored for that individual at the time of enrollment. Sophisticated matching algorithms either verify or deny the individual’s claim. Currently, within the criminal justice system, biometric technologies are primarily used to provide identification of an individual or a criminal suspect.

Presently, biometric technologies are being deployed sparingly throughout the United States for additional criminal justice purposes. For example, in the Salt Lake City area, mobile identification systems interface with database systems such as the AFIS that allow law enforcement officers to scan and capture fingerprints of an individual on a handheld mobile identification device. Via a wireless connection, the mobile identification system communicates with the AFIS for comparing and matching identification. This system was also deployed by the Ontario Police Department in southern California with spectacular results. In many correctional facilities, biometric technologies provide access control mechanisms for both employees and inmates. Meanwhile, another correctional facility currently uses biometric technologies to scan visitors as they enter and leave the facility. Furthermore, as a result of the 9/11 events, biometric devices will soon be deployed at every port of entry into the US.

We believe that the capability of biometric technologies to authenticate and verify an individual’s identity (i.e. verification) based on a previous enrollment to be significantly relevant, but perhaps overlooked, in preserving evidentiary value and raising the bar for collecting and tracking physical and digital evidence. More specifically, we believe the implementation of a mobile fingerprint biometric device in the field, interfaced with advanced communication and security technologies, can directly bind the ‘who’, ‘what’, ‘where’, ‘when’, and ‘how’ questions addressed within proper chain of custody procedures. Although we envision the application of biometrics in many other areas of the criminal justice system, we turn our attentions specifically to the chain of custody. Not only have criminal methods changed dramatically, but the methods of collecting, marking, storing, and maintaining evidence trails have changed remarkably as well. Law enforcement must continue to evolve and consider the benefits of innovative, technological solutions.

The chain of custody encompasses a number of ‘who’ questions. Who collected the evidence? Who took possession of it? Who took it out of storage? The use of a biometric technology can bind an identity to the question of “whom” and initiate a number of other computerized events to ensure integrity of evidentiary collection, preservation, and tracking steps. Upon successful verification of a law enforcement officer’s biometric, a number of processes could be subsequently initiated. For example, upon successful verification, a report that is typed on a laptop or written on an electronic tablet machine could be sealed with the verified officer’s identity, time stamped, encrypted, and subsequently transmitted to the station laboratory server for filing. Furthermore, biometric applications can secure access control within the forensic evidence storage room. Upon the request of a piece of evidence, a biometric will be verified, digitally time stamped, and electronically logged. Again, upon return of the piece of evidence, the biometric will be verified, digitally time stamped, and electronically logged. Biometrics can also be utilized for separation of duties during the collection and documentation of evidence at the crime scene; two biometrics could be used, one for the officer collecting evidence, and the

12 http://www.necsolutions-am.com/idsolutions/download/palmprint/palmprint.html
other for the officer documenting the collecting procedure. Upon successful verification of both identification credentials, the above detailed events of sealing, time stamping, encrypting, and transmitting the document electronically will occur.

Basically, biometrics can be used wherever hand signatures are currently required throughout the chain of custody procedure. Additionally, the use of biometrics can be appropriately combined with other computer technologies in use by law enforcement such as digital signatures, checksums, hash values, time stamping, and digital imaging. Eventually, we envision a paperless criminal investigation procedure. As the American society continues to progressively become paperless, sophisticated computer technologies will relieve law enforcement officers of many mundane and redundant duties, thereby allowing them to focus primarily upon the investigation at hand. Eventually, a biometric will be used to bind identity to and digitally time stamp and seal digital photographs of the crime scene. Videos of the crime scene will be secured using a biometric to bind identity and generate a digital time stamp, or hand sketches of the crime scene can be electronically scanned into a computer, and again sealed, signed, and delivered, all via a successful biometric verification. As with any new technologies, biometric technologies are not without their disadvantages as well as their advantages; and innovative ideas are not without their risks as well as their benefits.

The implementation of biometric technologies within the criminal justice system will not take place overnight. Although biometric devices are becoming significantly cheaper, efficient, and reliable, often these same devices can be very intimidating to the first time user. Fortunately, as deployment of the devices continue, users should become increasingly more comfortable with them. An additional controversy surrounding the use of biometric devices includes the concern of privacy. This is a debate that will continue to be waged between two

13 http://www.crime-scene-investigator.net/nighttime.html
14 http://www.sw.nec.co.jp/english/pid_e/mechanism.html
extremes of political ideals, however biometric technologies do in fact, provide a number of features for securing an individual’s privacy. Although each biometric device deploys individual security mechanisms, fingerprint devices and methodologies do not save a copy of an individual’s fingerprint and therefore privacy cannot be raped. As stated earlier in this article, the only thing stored from an individual’s fingerprint is a template. The template merely represents a mathematical, digitized representation of an individual’s minutiae points, and in more cases than not, the vendor encrypts the template in the process. Also, as many biometric vendors continue to provide comprehensive software development kits (SDKs) and application program interfaces (APIs), the development of user-friendly, reliable, and efficient biometric applications is within reach. In fact, a recently published technical study by WetStone Technologies, Inc., on the integration opportunities for biometrics in information assurance resulted in the successful development of a biometric security mechanism. The commercial name of this product is Time Lock™ Biometric. This product is a Microsoft® Windows plug-in that relies on a successful biometric verification to generate a digital timestamp and hash value for a Microsoft Word document. Overall, there are varying degrees of risks and benefits specific to the choice of biometric technology and the actual biometric to be used (i.e. fingerprint, iris, voice, signature), but we do not expect that implementation of biometric technologies within the criminal justice system will be deployed without a comprehensive investigation and testing of our proposed utilization of mobile fingerprint devices. We are sure however, that as the criminal continues to advance by embracing new, innovative technologies, that it would be unrealistic and illogical that our criminal justice system and law enforcement officers weren’t also provided with the efficiency, reliability, and benefits of innovative highly technical crime-fighting solutions.

With the advent of the computer criminal, and a suspicious eye turned inward upon America’s law enforcement officers, the past decade has spawned a requisite necessity for law enforcement to ensure the integrity of evidentiary value, from the initial collection of evidence throughout the complete criminal justice system. Since the erroneous handling of the O.J. Simpson criminal case, and subsequent mockery, law enforcement was compelled to consider the result of not successfully preserving the integrity of the chain of custody. The implementation of biometric technologies to bind identification to the movement of evidence from one pair of hands to the next represents a pivotal idea for ensuring the integrity of the evidence (and chain of custody) remains intact, thereby mitigating erroneous processes and allowing the criminal justice system to function as our founding fathers had envisioned, to provide justice for all.