Summer 8-2013

Are Fingerprints Really Individualized Evidence? A Meta-Analytic Study

Jonathan Dillon Barber
University of Southern Mississippi

The University of Southern Mississippi

ARE FINGERPRINTS REALLY INDIVIDUALIZED EVIDENCE?
A META-ANALYTIC STUDY

by

Jonathan Dillon Barber

A Thesis
Submitted to the Graduate School
of The University of Southern Mississippi
in Partial Fulfillment of the Requirements
for the Degree of Master of Science

Approved:

Dean of the Graduate School

August 2013

ABSTRACT

ARE FINGERPRINTS REALLY INDIVIDUALIZED EVIDENCE?

A META-ANALYTIC STUDY

by Jonathan Dillon Barber

August 2013

In recent years, there have been many academics that have challenged the legitimacy of fingerprints as a source of individualized evidence. They have also questioned the experts that analyze fingerprints and the methods they use. There have been recent cases where judges have questioned the foundation of fingerprinting and dismissed fingerprints as evidence. This meta-analytic study brings together opinions, cases, and studies that focus on the foundation, evolution, and technological advancements of fingerprinting.

ACKNOWLEDGMENTS

The writer would like to thank the thesis director, Dr. Kuppareddi Balamurugan, and the other committee members, Dr. Dean Bertram and Dr. John Bishop. I would like to thank Dr. Kuppareddi Balamurugan for guiding me and helping me throughout the writing of this thesis. I would also like to thank Dr. John Bishop for guiding me through this style of research, a style I was not familiar before this thesis. Finally, I would like to thank Dr. Dean Bertram for sharing his expertise in the field of fingerprinting.

TABLE OF CONTENTS

ABSTRACT ii

ACKNOWLEDGMENTS iii

LIST OF ILLUSTRATIONS v

LIST OF ABBREVIATIONS vi

CHAPTER

I. INTRODUCTION 1

II. OBJECTIVES OF THE STUDY 3

III. HISTORY OF FINGERPRINTING 4

IV. ANALYZING A FINGERPRINTING 9

V. SAMPLE OF STUDIES 16

VI. THE RELIABILITY OF FINGERPRINTS 18

VII. FINGERPRINTING TECHNOLOGY AND ADVANCEMENTS 27

VIII. HUMAN ERROR IN FINGERPRINTING 37

IX. CONCLUSION 47

REFERENCES 51

LIST OF ILLUSTRATIONS

Figure

1. Examples of the three categories of fingerprints.....11

2. Example of a minutiae-based biometric scanner. Left image is a mapped fingerprint image. Right image is the minutiae map of the left image.....32

3. Examples of three prints analyzed by a pore-based system 34

LIST OF ABBREVIATIONS

Class Evidence: Evidence that can only be linked with a group

Delta: the point on a ridge nearest to the center of the area of divergence of the lines of a fingerprint; the delta area is a triangular area where the lines radiate in three directions

Friction Ridges: raised portions of skin at the ends of the fingers that form a fingerprint

Individualized Evidence: Evidence that ties a single source to the crime scene

Known Print: a fingerprint which has a known origin; usually taken from individuals for a particular purpose

Latent Print: a fingerprint that is barely visible or invisible to the naked eye; found at a crime scene

Live Scan: the instrument and technology used to gather fingerprints; the prints are then uploaded to a database

Minutiae: a feature of a fingerprint used for comparison

Ridge Count: the number of ridges between the core and the delta of a loop pattern; used to quickly tell if two prints are from the same source

Unknown Print: a fingerprint that does not have a known source; collected from a crime scene

CHAPTER I

INTRODUCTION

For over a century, fingerprint analysis has been a beloved method of proving whether or not a person was innocent or guilty of a crime. Since 1902, fingerprints have been a staple in American law, and since then databases have been created to store more than 120 million fingerprint profiles. The belief that no two people share the same fingerprints has been stitched into this field since the very beginning, but is that really the case? A common comparison to fingerprints has always been the belief that no two snowflakes are alike but this was disproven in 1988 when a scientist found two sets of snowflakes that fell during a Wisconsin snowstorm were identical (Russell, 2012, n.p.). This belief, which had been around for centuries, was suddenly flipped upside-down. So, should we apply this belief to fingerprints?

In the 21st century, faith has been almost completely eliminated. Scientific certainty is what the world relies on (Cole, 2001). Considering that technology has advanced drastically since the early 1900s, how can we be sure that everyone on the face of the planet has different fingerprints? In a time of scientific advancement, people have been questioning this very belief. Television programs such as CSI and NCIS have given the public a distorted view of fingerprinting. These programs show that a fingerprint can be entered into a computer, and the computer will display a perfect match. That is not the case in real life. The computer gives a list of possible matches, and a qualified fingerprint examiner looks at the given prints to see if any of them match the unknown print. So what gives a person, even though they have been deemed qualified, the right to say beyond a shadow of a doubt that the person identified as the source of the fingerprint

is the only person in the world that could have produced the fingerprint found at the scene? Has the examiner compared the unknown print to everyone in the world? Has the examiner used a database that holds every print of every person in the world? The answer is simply, no (Cole, 2001). A great example of this is the case of an Oregon resident named Brandon Mayfield who was accused of being the Madrid train bomber by many top FBI investigators. The investigators claimed they found a fingerprint at the scene that matched Mayfield. Spanish authorities then discovered that the print actually belonged to a man named Ouhnane Daoud. FBI officials had to apologize for labeling Mayfield as the perpetrator (Russell, 2012). There are many other instances in the last few years that show how fingerprints can look very similar, especially when you have databases that use fingerprints from all over the world. Now that almost the entire world has been linked by databases, it is becoming more and more likely that a mistake will be made due to a striking resemblance between two fingerprints (Russell, 2012).

Many of the most respected names in fingerprinting have been debating the validity of fingerprints for decades. Some argue that two people cannot have the same fingerprints, so a match means that the person from whom the known print was gathered is the only person that could have left that print at the scene. Other forensic specialists have argued that when forensic scientists use fingerprints in a court case they should present the data similar to how DNA is presented. What is the probability that the defendant is the source of the fingerprint? (Pankanti, 2002). This meta-analytic review will bring together the opinions of the best minds in the field of fingerprinting as well as cases that have weighed heavily on fingerprint evidence.

CHAPTER II

OBJECTIVES OF THE STUDY

The main topics that will be discussed throughout this meta-analysis are: how reliable are fingerprints in today's criminal justice system (using thoughts and opinions from top minds such as Simon Cole along with cases that have been affected by fingerprint evidence), what role have the advancements in technology played in the field of fingerprinting, and how can human error affect the analysis of fingerprint evidence?

CHAPTER III

HISTORY OF FINGERPRINTING

To appreciate the arguments and debates that have been driven by so many people during the last few decades, an understanding of the history of fingerprinting is essential. The history of fingerprinting spans not only time but also many countries. An impressive artifact was found that showed fingerprints being used on contracts in ancient Babylon, and thumb prints being used on clay seals in ancient China. This shows that humans have revered fingerprints for not just a couple of centuries but for millennia. The Babylonians and Chinese may not have known the importance of what they were using, but they were intelligent enough to recognize the patterns that our fingers possessed. In 1686, a professor by the name of Marcello Malpighi identified ridges, loops, and spirals in his paper. This was the first recording of multiple patterns of fingerprints, but he did not identify that they had any significance. This was just a stepping stone in the recognition of the importance of fingerprints. Realizing that ridged skin "increases friction between an object and the skin's surface" (Barnes, 2011, p. 9) later led to the recognition that these ridges leave something special behind on the object that they touch. It wasn't until the 19th century that the importance of fingerprint patterns would be realized (Barnes, 2011).

The 1800's was the beginning of the importance of fingerprints. In 1823, a Prussian professor named Johannes Purkinje wrote a thesis describing nine different fingerprint patterns (Barnes, 2011). The first uses were actually used because of personal beliefs, not because of scientific reasons. The first time fingerprints were used as a form of identification was in 1858 in England. Sir William James Herschel had a print of his

entire hand placed on a contract. On later contracts he only used prints from his index and middle fingers. It was believed that the contract held more power if the person did not just sign it but also placed a print of a part of them on the contract. This was the beginning of fingerprints as a form of identification even though it was not scientifically grounded. In the 1870s, a British surgeon named Dr. Henry Faulds recognized that fingerprints could be used as means of identification. This was the first claim that fingerprints can be used for identification that was based on science. In 1880, Dr. Faulds wrote an article that discussed how to obtain fingerprints using ink. He even stated in one of his books that "when bloody finger marks or impressions on clay, glass, etc. exist, they may lead to the scientific identification of criminals" (Faulds, 1880, p. 12). This statement would lead to a dramatic change in criminal justice. Gavan Tredoux (2003) states that Faulds "gave two concrete instances where he had used prints forensically to establish the identity of people at crime scenes" (n.p.). These are some of the first recorded instances where prints were examined at a crime scene. One of the most important names in the history of fingerprinting is Sir Francis Galton. Sir Galton wrote a book in 1892 titled *Fingerprinting*. In this book he described the first classification system for fingerprints called Galton's details. The same year the book was released, an Argentine policeman named Juan Vucetich made the first ever criminal fingerprint identification. (Barnes, 2011)

The 1900's was the century when fingerprints became a critical part of identification. Before this, a system known as the Bertillon system was used to measure the physical dimensions of someone's body such as the length of the left foot and the length of the forearm from the elbow to the end of the middle finger. These

measurements were used as a classification system in prison systems to help identify anyone who had been incarcerated. This system was used for decades until a phenomenal case challenged its credibility (Barnes, 2011). In 1903, a man named Will West was incarcerated in a federal prison in Leavenworth, Kansas. While being booked like all inmates, it was discovered that his body measurements and even his photographs had a remarkable resemblance with another inmate by the name of William West. When this discovery was made, many prison systems turned to a new and promising method of identification, fingerprints. This case "helped bring in the era of fingerprint identification" (Thornhill, 2011, n.p.). As the popularity of fingerprints continued to rise, the United State Army began using them in 1905. Also in the same year, the Bureau of Criminal Identification was created. This bureau provided a place for a collection of fingerprint cards to be kept. For the next 25 years many law enforcement agencies submitted copies of their fingerprint cards to this bureau. In 1915, an inspector in Oakland, California by the name of Harry Caldwell wrote to many other inspectors pushing for an organization to be formed that would push the advancement of the identification profession. Later in the same year, several of these inspectors created the International Association for Criminal Identification. In 1918, this organization was renamed the International Association for Identification. This association is still the premiere organization for fingerprint examiners across the world. In 1918, Edmond Locard determined that for two fingerprints to be deemed a match there should be twelve points that are identical. In 1924, the Identification Division of the FBI was established. They had processed over 100 million fingerprint cards by 1946, and this number jumped to 200 million by 1971. Once the Automated Fingerprint Identification System (AFIS)

was put into place, these cards were uploaded to the database. It was found that many of the cards were duplicates, so the number of profiles was reduced to 25 to 30 million criminals. A huge addition to the field of fingerprinting came in 1977 when the International Association for Identification created the world's first certification program for fingerprint analysts. Known as the Latent Print Certification Board, it has tested thousands of analysts. This board challenged the claim that fingerprint experts never make mistakes in fingerprint comparison. Instead, they know that mistakes happen, and these mistakes should be addressed by the board. In 1997, the Department of Justice began using the Live Scan system, a system that would make the process of background checks requiring fingerprints automated. It was not until three years later that the Department of Justice requested that Live Scan be used to collect fingerprints instead of the traditional method of ink cards. This was a major step in the advancement of technology being used in fingerprint identification (Barnes, 2011).

The 21st century has seen the use of fingerprint identification go farther than anyone could have thought possible. The Live Scan system now has millions of fingerprint profiles that have been uploaded to AFIS (Barnes, 2011). Using fingerprints to identify criminals is not the only use for fingerprints anymore. Fingerprint scanners have become a very popular way to implement security measures. They became very popular with companies who wanted a way to keep out people other than their employees. This provided a huge upgrade in protecting sensitive information. Not only is information protected by these devices, money is also protected. Banks have started using these identification systems to stop thieves from breaking into their safes. But over the last few years it has become much more common with the public. Now the average

person can purchase a fingerprint scanner for their computer and use their fingerprints as their passwords. Some commercially available safes have these scanners installed so the owner does not have to use the traditional method of using a combination of numbers. There is one ironic thing about the inclusion of this technology in this analysis considering that this analysis focuses on the debate that fingerprints should or should not be seen as unique characteristics. This technology relies on the belief that no two fingerprints are the same, but what if two people had the same print and they both somehow tried to use the same fingerprint scanner? Wouldn't that defeat the purpose of the system? This system obviously favors one side of the argument of this analysis. There has not been a reported case of someone gaining access to an area because the system confused their fingerprint with the fingerprint of the actual person whose profile is stored in the system's database. Is this because the system eliminates the human error aspect of comparison? That is a question that really cannot be answered, but it is one perspective that has been brought up over the last few years. Ellis-Christensen (2003) stated, "Though fingerprints cannot be identical, they can in fact be very similar" (n.p.). Could two fingerprints share the same category and subcategory but differ only because of a few different minutiae? There was a case where a son unlocked his father's computer using his own fingerprint when the registered print was actually his father's. Does this show the flaw not only in fingerprint scanners, but the belief of everyone having unique fingerprints? Considering how quickly technology has evolved in the 21st century, the technology used for fingerprinting will inevitably become more efficient and more powerful (Barnes, 2011).

CHAPTER IV

ANALYZING A FINGERPRINT

Almost everyone knows what a fingerprint looks like, but how is one analyzed after it has been collected? What do you look for? First, knowing what a fingerprint is formed by is crucial. Everyone that has fingers has fingerprints. They are made up of raised portions of the skin on the ends of the fingers called friction ridges. These ridges form a very complex pattern on each finger. Friction ridges are flexible, so taking prints from the same finger twice may yield slight alterations in the print itself. Once a fingerprint is collected, it is analyzed to determine what category it belongs to. There are three categories that all fingerprints fall under: arch, loop, and whorl. It has been determined that 70% of fingerprints are loops, 25% are whorls, and 5% are arches. Each of these categories has subcategories. Each category has certain elements that are used for analysis and comparison. One element that is shared by loops and whorls is a delta. This is a vital element in each pattern, but they are used in different ways. A delta is identified by the point of the print nearest to the center where the ridges diverge in three different directions. Discussed below is their specific purpose in the two patterns in which they are used.

Loop patterns have ridges that begin on one side of the pattern, loop up, and come back to the same side they started from. Loops are broken into radial loops and ulnar loops. The way they are differentiated is by which bone in the forearm the print leans toward: the radius or the ulna. The center of the print, also known as the core, looks as if multiple ridges wrap around it. These ridges play a crucial role in identification. Once the delta is established, a ridge count is performed. The examiner counts how many

ridges are present between the core and the delta. If one print has a ridge count of twelve and one has a ridge count of fourteen, then they are not a match (Franklin, 2003).

Whorls have a circular pattern. The category is broken into four subcategories: plain, central pocket loop, double loop, and accidental. A plain whorl has a large circular pattern. A central pocket loop whorl has a small, tight circular pattern. What differentiates the two? There are two deltas present in a whorl pattern. If the deltas are below the bottom of the circular pattern, then it is classified as a central pocket loop whorl. If the deltas lie above the bottom of the circular pattern, then it is a plain whorl. A double loop whorl is a pattern that contains two loops, one pointing up and one pointing down. This pattern is sometimes mistaken as a loop pattern because the loop that points down is overlooked. An accidental whorl is a pattern that consists of two different types of patterns which is very rare (Franklin, 2003).

Arches are identified by the manner in which the ridges flow from one side of the print to the other. There are no deltas in an arch pattern. There are two subcategories of arches: plain and tented. A plain arch has lines that flow smoothly across the pattern. There are no major peaks in a plain arch, only a smooth rolling formation. It resembles a calm wave of the ocean. A tented arch has a very pronounced peak in the center of the pattern. The central line will be at a very distinct angle from the other lines, sometimes causing nearly ninety degree angles. Arches are the rarest form of fingerprints (Franklin, 2003). Figure 1 shows diagrams of the three categories of fingerprints.

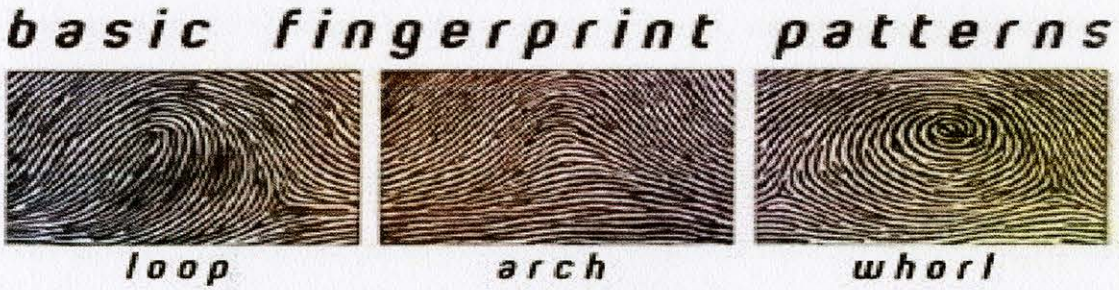

Figure 1. Examples of the three categories of fingerprints. Adapted from "Fingerprints used in Forensic Investigations" by Diana Gurdoglanyan, *Bronx Science*, 2001.

Once the category and subcategory of a print are identified, it must be analyzed even further. The main identifiers that are used by fingerprint examiners are called minutiae. These characteristics have different shapes and features. One example is a bifurcation. This is identified by one ridge splitting into two ridges. It appears in the shape of a "Y". This is a commonly used minutia because it is easily identified. Another example is an island. This is a circular ridge that is surrounded by other ridges. The reason it is called an island is because it looks like an island in the middle of the ocean. Another form of minutiae is a short ridge. It is a very short ridge that is not connected to another ridge. This is usually one of the harder minutiae to identify because deciding what makes a ridge "short" can be different between fingerprint examiners. Minutiae are not the only markers used by examiners. If someone has a scar on their finger from some kind of trauma that occurred in the past, it can be used to identify them. The size and location of scars are unique, so they can be used as an aid in comparison (Prabhakar, 2002).

Now that the patterns have been described, knowing how fingerprints are recovered from a crime scene can be helpful in understanding what a latent print is and how they are handled. A latent print is a fingerprint that is found at a crime scene. It is barely visible to the naked eye. They are found at crime scenes where someone has

touched an object with their fingers. A mixture of water and salt from sweat found on the skin of the fingers leaves an impression of the ridges that are on the ends of the fingers. There are different methods that are used for recovering fingerprints from different surfaces. The surface that comes to everyone's mind is glass. Collecting evidence that is glass has to be done very carefully because placing it in a bag could damage the fingerprint. It must be placed in something that will keep the glass surface from coming into contact with anything. The best way to recover fingerprints from a glass surface is to place the glass object in a vapor chamber where cyanoacrylate, more commonly known as super glue, is vaporized. This chemical adheres to the print showing the ridge detail so that it can be analyzed. Dusting is the most recognized form of revealing prints, but using powder on a glass surface could damage the fingerprint by smearing it. Dusting is used more for porous surfaces such as paper or wood. Powder comes in two types: volcanic and magnetic. Either can be used to lightly go over the fingerprints so that the powder adheres to the print. This reveals the ridge detail so the print can be processed and analyzed. But how can you see the fingerprint if the surface is dark? Using a fluorescent powder will allow the fingerprint to be seen with an alternate light source. Using an alternate light source such as ultraviolet light will allow the fingerprint to be seen very brightly even if the surface is dark. Also, using a fluorescent powder and an alternate light source will greatly increase the chance that DNA testing can be conducted on the fingerprint because it does not damage the carbon makeup of the print (Sumayao, 2003).

Known prints are collected by qualified experts from criminals who have been incarcerated or from people who are under suspicion of a crime. One method of

collecting these fingerprints is with ink. Ink is used by rolling the end of the finger on an inkpad then rolling that finger on a white fingerprint card. Each fingerprint is rolled individually, and then all four fingers are done together followed by the thumbs individually done. When the fingerprints are done together and the thumbs are done the second time, they are pressed down not rolled. This is because if their fingerprint is found somewhere there is a much greater chance that they placed their finger on the object, not rolled it on the object. Using ink on a fingerprint card is the more consistent method of collecting fingerprints from someone, but there is another method that is a little less messy. An electronic program called Live Scan collects fingerprints using a computer station. The end of the finger is placed on the machine, and the machine collects the print. Once the fingerprint has been collected, it is transmitted to the desired department or agency. The prints are stored along with the profile information of the person who is the source of the prints. Live Scan does have numerous advantages over the traditional method of ink. Once fingerprints are entered into the system, results of a search can return within a 72 hour period. Another advantage is that the fingerprints can be sent directly to AFIS. Also, if fingerprints from a suspect are needed from a department or agency far away, those prints can be immediately sent to them through their Live Scan system. This transfer only takes minutes, whereas sending an agency fingerprint ink cards would take days. Using Live Scan may be less messy than using ink, but it does have its drawbacks. The computer may not collect the fingerprint properly, so scanning the same fingerprint several times may be necessary to collect a suitable print. Live Scan is also much more costly than ink.

A large majority of fingerprint examiners use a system to analyze fingerprints. It has been deemed the fingerprinting equivalent to the scientific method. The acronym that is followed by fingerprint examiners is ACE-V which stands for Analyze, Compare, Evaluate, and Verify. First, you analyze the unknown print and known print that you were given to see if they resemble each other. This is where the examiner uses the three main categories. Are both of the fingerprints an arch, loop or whorl, or do they have two different patterns? If the two fingerprints have different patterns, the examiner can rule that they are not a match. If they share the same pattern, the examiner then breaks down the prints even further. The examiner identifies the delta or deltas if they are loop or whorl patterns. If they are loops, the examiner then identifies the core of the pattern and performs a ridge count. If the two ridge counts differ, then it can be concluded that the two prints are not from the same source. If they do match, then the analysis continues. Next, the examiner looks for any minutiae that may be used as identification markers. Bifurcations, short ridges, islands, and ridge endings are major minutiae that are used by fingerprint experts. But how many of these markers should match on the two fingerprints to conclude that they are a match? In 1918, Edmond Locard stated that twelve points should match for there to be a positive identification (Barnes, 2011), but different agencies and companies have different standards for how many minutiae matches must be found to rule that the two prints match. That is one common argument about the validity of some positive identifications. Since there is no set number that is accepted by everyone, what gives someone the right to choose their own number to go by? After these minutiae are marked on each print, they are compared. Now the examiner evaluates his/her findings. Do the two prints match? Is there enough information to reach a

conclusion? In many instances, fingerprints that are recovered from crime scenes are in terrible condition. They may be smeared, only part of a print, or prints may be overlapped causing skewed evidence. In cases where the print recovered from a crime scene is not of high quality, it may be determined that a conclusion cannot be reached. This gives the fingerprint examiner three possibilities: a match, not a match, or inconclusive. Once the examiner makes the decision that the prints do or do not match or their finding is inconclusive, the prints and findings are transferred to someone else for verification. Usually someone who is also a qualified examiner examines the findings to see if the decision was the correct one. This system has been used for decades even though its validity has been questioned by many. Fingerprint experts continue to use it because it has proven to be a very effective and efficient way to analyze and compare fingerprints (Triplett, 2006).

CHAPTER V

SAMPLE OF STUDIES

There are countless articles that have been written about fingerprinting and its validity. Some people defend it, and some try to expose the flaws that lie within the field. This meta-analytic review is based on numerous articles, journal entries, and accounts written by some of the most respected names in the field of fingerprinting. Some defend the absolute certainty of fingerprinting while others are trying to convince others that scientific advancements have flipped the world of fingerprinting upside-down. All of these opinions have been gathered into this review so they can be compared to and contrasted against each other. Not only does this meta-analysis contain highly respected views from the top minds in the field of fingerprinting, it also contains cases that have been affected by fingerprint evidence. Considering that fingerprints have been used in the court of law for over a century, there are numerous cases that have been decided by the analysis of fingerprints. A great example of this is the Madrid train bombing (Russell, 2012). Throughout this time there has also been much advancement in the field of fingerprinting ranging from techniques used to collect fingerprints to technology that is used to help compare prints. These advancements will also be discussed throughout this review. Another topic that will be discussed is the validity of comparisons made by human eyes. There are forensic scientists that have the label of *fingerprint expert*. What makes them *experts*? Are they so well trained that they will never make a mistake? Human error has always been a debate among forensic scientists, and this review contains debates and examples of how a person can affect the data gathered from fingerprint analysis (Cole, 2005).In order to understand these cases and opinions that will be within

this analysis, knowing what a fingerprint is will make the reading much more enjoyable. The three main categories of fingerprints have been described and broken down into their subcategories. Also, the markers that are used for fingerprint comparison are described. This will show what fingerprint experts look for when analyzing and comparing prints (Franklin, 2003). The history of fingerprinting is also discussed so that the reader can have an appreciation of the evolution of the field as they read this meta-analysis. Some of the information about the field is highly fascinating, so it may add to the experience of this analysis. Shedding light on the hot topic of absolute certainty in fingerprinting is the overall objective of this meta-analysis, so gathering the most credible and relevant material is of the utmost importance.

CHAPTER VI

THE RELIABILITY OF FINGERPRINTS

Over the last century, fingerprint analysts have stuck by the belief that no two fingerprints are the same. Analysts continue to testify with absolute certainty that fingerprints are unique and a definitive way of identifying someone (Cole, 2009). Is there scientific proof that backs up this claim? Have there been rigorous tests performed to see if this assertion is scientifically accurate? (Russell, 2012). Jennifer Mnookin (2008) makes an interesting point when she discusses how two different conclusions could be reached to these questions. If someone were to investigate the reliability of fingerprinting using sources only from judicial rulings it would most likely seem that fingerprinting is a reliable form of evidence because it is accepted by the *relevant scientific community*. Esther Ingles-Arkell (2012) mentions a case where a pair of twins were arrested for stealing 10,000 pounds worth of watches, but neither one of them were convicted because they both claimed they were home at the time of the robbery. Blood was found at the scene, but it was not helpful because DNA of identical twins is the same. Ingles-Arkell states that "if either one of them had left a fingerprint on the glass, the police would have been able to arrest the guilty twin" (n.p.). Because no fingerprints were found at the scene, both twins walked. Some people do not feel the same way as Ingles-Arkell. Robert Epstein made a bold statement that shocked the courtroom, "...since the reliability of fingerprint matching had never been tested or proven, it should be barred as evidence from the courtroom" (Eaglin, 2009, n.p.).

A senior judge in England also challenged the reliability of fingerprinting because of the "recent cases of innocent people being wrongly singled out by fingerprint

evidence" (Edwards, 2010, n.p.). This judge, Lord Justice Leveson, stated that research needed to be done to prove that fingerprinting is "'robust' and reliable" (Edwards, 2010, n.p.). Although some people have been wrongly accused because of fingerprint evidence, there are still many instances where fingerprints were used to help convict someone who was actually guilty of the crime they were charged for. In 2000, a woman named Shervie Anne Elliot was found dead at her place of employment, ABC Liquors in Jacksonville, Florida. Fingerprints were found on a receipt pouch that belonged to the liquor store, and after analysis it was determined that the fingerprints matched a man named Richard McCoy, a man who was turned in by his girlfriend for the murder and robbery. It was documented that "ABC Liquors store pouches were 'kept within the store office at all times, and only store managers were involved with the pouches'" (Richard McCoy vs. State of Florida, 2013, p. 18). This contradicted McCoy's claim later in the trial that he found the pouch in a parking lot and mailed it to the ABC Liquor's main office. McCoy claimed that he found the pouch in a parking lot he was in after leaving a Days Inn. The police investigated the hotel claim, and it was discovered that the room McCoy claimed to have spent the night in was reserved by someone else that night. One of the arguments made by the prosecution is that "fingerprints are not subject to human error or mistakes" (Richard McCoy vs. State of Florida, 2013, p. 9).

Michael Mears (2003) argues that "fingerprint identification is reliable because it has been accepted in the scientific community," but he also notes that he believes this "'scientific community' is limited to law enforcement" (p. 29). Mears continues to show his displeasure of the fact that fingerprints are accepted as evidence by saying, "Although identification by fingerprint comparison may be a scientific hypothesis, it is not a valid,

proven scientifically reliable theory, and the courts of law should not recognize it as such" (p. 30). It is clear the Mears would like to see fingerprinting banned as evidence completely, but what would that say about our criminal justice system? Fingerprints have been used for over 100 years and have been crucial pieces of evidence in many cases, so does that leave our entire criminal justice system vulnerable to scrutiny? Mears continues by comparing fingerprinting to hypnosis and polygraphs. Hypnosis is "well accepted for psychological research and psychotherapy" (p. 30), but using it to get a testimony is inadmissible in court. Polygraphs "have a number of accepted applications in physiological research and medicine" (p. 30), but using a polygraph session in court is not allowed. Do these comparisons make sense? What truly makes fingerprinting more reliable than methods such as hypnosis and polygraphs when they have shown to be very important scientifically?

Considering that fingerprint analysts follow a popular method (ACE-V) that some compare to the scientific method, it makes fingerprinting appear highly dependable, and the state and federal courts have judicial faith in this process of identification. On the other hand, if someone were to investigate academic sources such as peer-reviewed articles it would seem like there are still many questions that need to be answered about fingerprinting. Unlike DNA evidence, there is no scientific model that fingerprint analysts follow. How many points of resemblance does it take to prove that the two prints are a match? It is completely up to the analyst to make this decision. So how can this be *scientific* when it is based on the preference of the analyst? (Mnookin, 2008). Lyn and Ralph Haber (2008) have gone as far as suggesting steps that could be taken to validate the method of fingerprinting known as ACE-V because they believe that this

method has yet to be tested. Haber and Haber also claim that the method is untestable at the moment, and "until the method is specified and endorsed, there is no method to test" (p. 93). If this statement is accurate, how can the judicial system rely on evidence that is produced by an analyst that claims he or she used this method? If the method itself is untestable, how can you use it to *test* evidence? Inman and Rudin (2001) state that "it is impossible to separate the analyst from the method" (n.p.), so is this the reason ACE-V is untestable? Mnookin (2008) agrees with Haber and Haber (2008) that ACE-V needs to be completely overhauled and more scientific. Even Cole (2009) believes that many forensic identification methods are starting to become criticized because the "many techniques lack basic validation" (p. 234). Spinney (2010) goes deeper into why the ACE-V method is unreliable. Spinney claims that the ACE-V method is *sloppy* by academic standards. One point Spinney (2010) touches on is the Verification step of the ACE-V method. Someone must verify that the first three steps were done correctly, but "the verifier often works in the same department as the first examiner and knows whose work he or she is checking" (Spinney, 2010, p. 345). Most scientists prefer some form of *independence*, but that is not the case in Spinney's illustration. Triplett (2006) makes a valid argument that the verification step is sometimes confused with confirmation, meaning that confirmation is "to uphold the initial examiner's conclusion" (p. 347). Triplett believes this step should focus on the "attempt to falsify the original examiner's conclusion or how it was arrived at" (p. 347).

Since the Daubert rule (Zonana, 1994) there have been multiple court cases where fingerprinting evidence was challenged because of the argument that there is a lack of scientific validity. Mnookin also shares her feelings about how courts accept fingerprint

evidence. She states, "... the argument some courts proffer that fingerprint is valid because it has survived a century of testing within the adversarial crucible is almost laughable" (Mnookin, 2008, p. 133). Do the courts and even law enforcement have a bias toward fingerprints because it has been used for so long? An interesting point made by Cole (2010) actually relates to DNA evidence found at a crime scene. Cole (2010) finds it troubling how DNA evidence is underused, stating that "...DNA profiling is conceived by police investigators as a tool for building evidence against a suspect identified by other means rather than as a means of generating a suspect by treating existing archives of genetic information as what have been called 'DNA intelligence databases'" (p. 376). Are fingerprints still valued more than DNA because fingerprints have been used for much longer? Inglis-Arkell (2012) makes an interesting claim that "... [fingerprints] came of age in an era well before our time, and were grandfathered in to the modern court system" (n.p.).

Leadbetter (2005) discussed an interesting case that helped fingerprinting gain popularity. This case was the Farrow Case in London, England in 1905. Mr. and Mrs. Farrow, managers at a hardware shop, were found brutally murdered at their business. The police found a metal cash box with one bloody fingerprint on it. After coming to the conclusion that the fingerprint did not belong to Mr. Farrow or Mrs. Farrow, it was determined that the fingerprint belonged to Alfred Stratton. Alfred and his brother Albert were convicted of murder and were hanged. What made this case special was the fact that it was the first British murder case to use fingerprints, and the fingerprint was the vital piece of evidence. Leadbetter (2005) defends fingerprinting stating, "Significantly, since those early days no better method of personal identification has yet been devised or

discovered…" (p. 3). Also, Leadbetter showed that he believes in DNA evidence, and that "It would be difficult to imagine any present-day police force functioning effectively without fingerprinting and DNA analysis in its crime-fighting armoury" (p. 3). There are many people that still believe in the validity of fingerprinting, but can their opinions help offset all of the criticism seen in recent years?

Hypothesis testing has been used for centuries because of its reliability. This type of testing has an error rate that is almost negligible, but no one has ever claimed that the error rate is zero (Triplett, 2006). If this is the case with one of the most beloved testing styles, how can fingerprint analysts claim that fingerprint identification has an error rate of zero? Wise (2004) talked about the case of *United States v Carlos Evan Llera Plaza*. Judge Pollack decided that fingerprint analysis did not meet the criteria established by the Daubert case. Judge Pollack was also unsatisfied with the error rate of zero because of a lack of documentation confirming the error rate. Cole (2005) also asks the question of "How can a process commit errors and yet be considered infallible" (p. 990)? Cole believes that fingerprint analysts continue to defend the infallibility of fingerprints because the analysts "isolate, minimize, and otherwise dismiss all exposed cases of error as 'special cases' or one-offs" (Cole, 2005, p. 991).

Another interesting point Cole brings to light is how fingerprint examiners defend the zero error rate when testifying. Fingerprint examiners "testify that the 'methodological error rate' is zero, but they do not testify that the 'practitioner error rate' is unknown" (Cole, 2005, p. 1037). Cole also states that there is not even an attempt to measure practitioner error rate because fingerprint examiners testify that the practitioner rate is basically negligible, and the courts have faith in it. Edwards (2010), who reported

on the reactions of Lord Justice Leveson in England to fingerprinting, reported that Lord Justice Leveson stated, "The language of certainty that examiners are forced to use hides a great deal of uncertainty, which greatly undermines the examiners' legitimacy" (n.p.). What does this imply for thousands of fingerprint examiners that have made their career on this claim? Lawson (2006) makes a comparison of fingerprint examiners to an eyewitness. Lawson states that:

> ...in the eyewitness context, the lay juror is more likely to believe a victim who is absolutely sure about the identity of her attacker over a victim who testifies less adamantly regarding identity. Yet, scientific studies of eyewitnesses' ability to correctly identify their true attacker support the opposite conclusion, and the victim who testifies she is '100% sure' about identity is no more often correct about the identity of her true assailant than the victim who testifies less adamantly. Therefore, the knowledge of this empirical fact, in the form of framework evidence contained in a special jury instruction, helps the jury to properly assess the victim's credibility and not overweigh her eyewitness identification testimony simply because she says she is 100% sure. (p. 62)

So does this statement by Lawson challenge the rights of the fingerprint experts to use the *100% sure* claim? Lawson goes on to suggest that courts should allow the defense the right to use the special jury instruction when fingerprints are involved in a case. Would this affect the reputation of fingerprinting?

Inman and Rudin (2001) state that "while not all evidence is either potentially or necessarily individualizable, the concept remains the hallmark of our profession" (n.p.). But are fingerprints really individualized evidence? There is one word that forensic

scientists link with individualization, and that word is uniqueness (Cole, 2009). Uniqueness is the belief that everything in the universe is different, and Inman and Rudin claim that "our belief that uniqueness is both attainable and existent is central to our work as forensic scientists" (p. 236). But Cole questions this belief for several reasons. He points out that no experiment has been done on today's databases to see if there are duplicates within the database. Cole also makes sure to explain that "such experiments cannot prove uniqueness; they can only establish that duplication is highly unlikely." Even if an experiment such as this was done, the fingerprints on the databases are just a small fraction of all of the fingerprints in the world (Cole, 2009). But Inman and Rudin make sure they state that "we must be clear that [uniqueness] is a belief, not a fact. Not only has it not been proved, it is unprovable" (n.p.). One reason uniqueness is accepted among scientists and the courts is because of the belief that nature never repeats itself (Cole, 2009). This belief has been accepted for millennia, but again it is not something that can really be proven. Michael Lynch, a professor of science and technology studies at Cornell University, was interviewed by David Brand (2002) about fingerprint evidence and DNA evidence. Lynch stated that "the courts are confusing the issue by making the identification with science so important. Whether fingerprinting is science or not is beside the point. The question is, is it good evidence" (n.p.)? Does this statement have a valid point? Although he shows some faith in fingerprinting, Lynch does show his concern that fingerprinting does not have probabilities. He would like to see fingerprinting adopt a system similar to DNA where "procedures for probability have been established" (n.p.). When talking about the belief that no two fingerprints are alike, Lynch states that "... since it's impossible to compare the fingerprints of everyone in the

world, this assumption still stands" (n.p.). Arguments have been made that since it is impossible for every fingerprint in the world to be analyzed it should not be assumed that everyone has different prints, but is Lynch making an argument for the contrary? Is he stating that fingerprint experts have the right to claim that no two prints are the same?

The thought of a probability model for fingerprinting has been a popular topic among critics, but the International Association of Identification has not accepted this model. The IAI stated that "probable or possible identification conclusions are outside the acceptable limits of the friction identification science" (Peterson et al., 2009, n.p.). How does this statement affect the potential for such a system? Considering how well-respected the IAI is, how can a probability system gain respect in the fingerprinting community?

Even though it is very rare that a criminal case has a pair of identical twins involved, how could the genetics of identical twins hinder a criminal investigation? In 2010, Lee Ferren reported that a man named Donald Smith was arrested for murder in 2008. Camera footage and DNA evidence seemed to clearly link Donald Smith with the murder, but he made a startling claim: it was his identical twin brother that committed the crime. After he made this claim, the police investigated his twin brother Ronald Smith. After analyzing the fingerprints found at the scene it was discovered that the prints matched Ronald Smith, not Donald Smith. Once presented with this evidence, Ronald admitted to the crime. Ferren shows how fingerprinting can pick up DNA's slack by stating, "In a justice system that often relies heavily on high-tech DNA testing, it was fingerprinting, a practice more than a century old, that succeeded where DNA failed" (Ferren, 2010, n.p.). Do cases like this show fingerprinting's legitimacy in court?

CHAPTER VII

FINGERPRINTING TECHNOLOGY AND ADVANCEMENTS

Technology continues to advance at an astounding rate, but what effects can this advancement have on the field of fingerprinting? Computers have become a part of everyday life, and Debbie Salter discussed how computers have begun to aid in the process of fingerprint identification. Computers have helped ease the duties of police officers when it comes to a suspect list by generating a list instead of officers tirelessly compiling a list of suspects. Computers also are "able to identify and classify more information than the capabilities of humans" (n.p.). Another ability of computers that Salter highlights is the "elimination of time issues and human error in classification and comparison" (n.p.). Do computers actually eliminate these problems? Dror, Wertheim, Fraser-Mackenzie, and Walajtys (2012) performed an experiment that tested this very question. Dror (2012) performed a study where fingerprint examiners analyzed fingerprints that were given to them by AFIS. Dror and his colleagues (2012) manipulated the order of the fingerprints to see if the examiners would be affected by the order (AFIS gives a list of fingerprints in which the most likely match is listed number one). This study was to see if the examiners would show bias because of the order of the fingerprints. Dror stated, "If AFIS rankings tend to be accurate, human examiners may experience efficiency gains by utilizing that information, and focusing their cognitive resources on the highest-ranking exemplars" (p. 350). Is it just human nature to focus more on the fingerprints that are most likely to match? Dror goes on to say, "There may also be too much of an examiner focus on the top prints in a ranked list, especially given the general psychological and cognitive bias to prefer the first choice" (p. 350). So how

effective is the relationship between the technology and the examiner? The results of Dror's study show that "The important and consistent result is that in both analyses, with and without the potential 'clerical errors,' the position in the AFIS list played a critical contributing role in the way examiners conduct their comparisons and conclusions" (p.350). Is there a way to modify AFIS's output so that it does not lead to bias errors made by the examiner? Dror believes that "It would be simple to modify AFIS's output to eliminate the examiners' knowledge of AFIS's ranking, by providing lists to examiners with prints in a random order." This is a great idea, but would past biases continue to creep in even if this change is made? Human beings are creatures of habit, so would the examiners still have the mindset that the first print on the list is the most probable for a match?

Another effect that was observed during Dror's study was comparison time. Since AFIS gives the list of possible matches in order of probability are the fingerprint examiners spending more time on some prints than others? Dror et al. (2012) hypothesized that if an examiner spent more time on a comparison it would lower the chance of an error being made. After analyzing the data it was discovered that "as the comparison time decreased, the likelihood of an error rate is increased" (p. 346). This does not answer the question asked, but Dror also ran an experiment that would answer it. He ran a second experiment that tested the comparison times were affected by the position of the "target matching print" (p. 346). The results showed a "significant statistical effect of target position on the comparison time of the target matching print" (p. 347). It was clear that the fingerprint at the top of the list was favored over all the other fingerprints, but in the study conducted by Dror the matching fingerprint was

placed in different positions of the AFIS lists. After the first two experiments had been run, two conclusions were reached: as comparison time decreased, the likelihood of an error rate increased; and the target print position had an effect on the comparison time. So what does it mean when these two results are put combined? Dror (2012) states that, "… when the target is in a position other than the top position, the examiners were more likely to make an error if they have decreased their comparison time. By contrast, when the examiners took a longer time for the comparison, the effect of the position of the candidate print had less of an effect on error rates" (p. 347). Considering this, what can laboratories and agencies do to assure that the error rates are kept at a bare minimum? How can the technology-human relationship be reformed so that the examiner does not show bias in any way to the data given by a system such as AFIS? In 2010, Dror collaborated with Jennifer Mnookin to study the challenges that arise from this relationship. They state, "If a technology is going to be used to its maximum potential, we must first understand the implications and consequences of using it and make whatever adaptations are necessary both to the technology and to the way humans work with it" (Dror & Mnookin, 2010, p. 47).

Dror and Mnookin (2010) believe that technology should bring about change in the way comparisons are performed. They state, "Put simply, the use of AFIS ought to change the way fingerprint experts conduct comparisons, and what they require in order to declare a 'match', because making identifications is simply not the same cognitive task as it was prior to the use of massive, automated computerized databases" (p. 51). But is this type of technology making the fingerprint examiner more obsolete as it advances? Some agencies have begun to only rely on AFIS to match fingerprints when it comes to

tenprints (a set of someone's ten fingerprints taken previously in an orderly fashion), completely removing a fingerprint examiner from the equation (known as *lights out* because the system can run while no one is at the office and the lights are out). This process allows AFIS to determine a *match* as long as it meets a certain threshold. Does this put too much faith in the technology? This may be true for the tenprint scenario, but what about when it comes to matching fingerprints that are found at a crime scene. Fingerprints found at a scene are rarely perfect and undamaged, so how does this affect the role of AFIS? Dror and Mnookin say that, "At present, for latent prints, AFIS' capabilities are thought not to surpass, or even to meet, those of human experts, and therefore no one currently advocates taking a fully 'lights out' approach to latent fingerprinting" (p. 52). The role of AFIS in latent fingerprinting is "collaborative" as it only aids the examiner by forming a list of possible matches. But could this collaboration lead to unforeseen problems within the technology-human relationship?

Dror and Mnookin (2010) feel that "not only is latent fingerprint identification not living up to its full potential but also that the chances for incorrect identifications have increased" (p. 54). In their article they suggest three areas that need revision when it comes to using AFIS. The first is examiners should modify their *decision threshold* when declaring a match. Dror and Mnookin speak of how examiners now have a database with millions of fingerprints to compare with, but before AFIS was available the examiner would only be analyzing a handful of fingerprints, mainly the fingerprints of people who were suspects in the crime. Considering the drastic escalation in the amount of fingerprints the examiners have to deal with, how should the examiners adjust? Dror and Mnookin (2010) state that, "When database size increases, the chances that some

print in the database will bear a high degree of resemblance to the latent in question also goes up" (p. 55). They compare this problem to how DNA is handled. If a DNA sample is found to have a probability of 1 in a million, how will that affect the results from a database search if the database has a very large amount of profiles? Dror and Mnookin write, "If the database is sufficiently large, it is likely that someone in the database will be a 'random' match – that is to say, someone who truly *does* have the same DNA markers at the tested loci, but is nonetheless *not* actually the person who left the biological sample at the crime scene" (p. 55). Now that so many fingerprints have been inputted into the AFIS, what does it mean for the error rate? Debbie Salter states that the accuracy of an AFIS search is "98-100%" (n.p.). If AFIS' error rate is 98% and an analysis is run for 60 million fingerprints, then that means 1.2 million fingerprints will be run through AFIS with an error. Dror and Mnookin state that, "[examiners] should require *more* evidence of similarity when making an AFIS match than they would require elsewhere." (Dror & Mnookin, 2010, p. 56)

One piece of technology that has become very popular in many aspects of today's world is the fingerprint scanner that is used as an access terminal to sensitive places. Instead of using a password to access things such as computers or sensitive rooms, this type of biometric scanner uses *physical* traits that stay with the individual (Uludag & Jain, 2004). Figure 2 shows an example of how the type of biometric scanner analyzes a fingerprint.

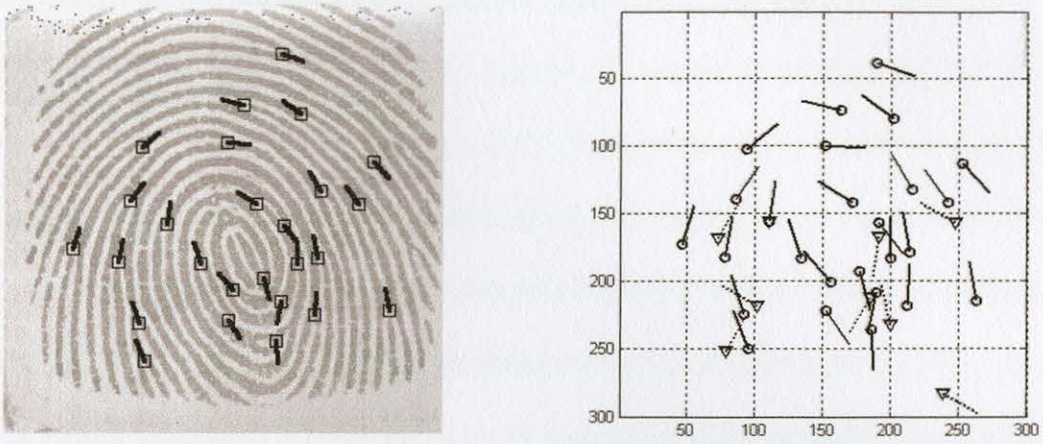

Figure 2. Example of a minutiae-based biometric scanner. Left image is a mapped fingerprint image. Right image is the minutiae map of the left image. Adapted from Umut Uludag& Anil Jain, Attacks on Biometric Systems: A Case Study in Fingerprints, *Michigan State University* (2004).

But is this technology safer than password-using technology? Someone can steal your password, but can someone steal your physical traits? Uludag and Jain performed a study on fingerprint scanners that use an algorithm to analyze minutiae patterns on fingerprints. Their objective was to see if *fooling* the system was possible. One theory they formulated was that someone could create a *fake biometric* such as a synthetic fingerprint that can be used to fool the system into thinking it is the real finger of someone who is granted access to that area. Uludag and Jain state that "Fake biometric submission to the sensor … is shown to be quite successful by several researchers" (p. 3). The reason this method is so effective is because it does not require the intruder to know the "digital limits of the biometric system," and "the digital protection mechanisms such as encryption, digital signature, hashing etc. are not applicable" (p. 3). The digital properties of the systems are much more difficult to fool but do not require as much time as creating a synthetic fingerprint. Uludag and Jain (2004) used a system that dealt with ridge information including "triplets associated with each minutia" (p. 7). The two

researchers came to the conclusion that the system used was "quite effective when breaking into accounts protected with templates composed of minutiae location and angle formation" (p. 11). It took an average of 271 attempts to get the system to register a positive identification, and the two researchers are "currently working on modified attack system with the aim of decreasing the number of attempts even further" (Uludag & Jain, 2004, p. 11). Can revealing the vulnerability of biometric systems be positive, or will it create more problems? Uludag and Jain recommended a few ways to protect from potential security threats. One solution they spoke about was to "block matching attempts if there are too many false matches in a given period of time" (p. 11). With the average of their tests being 271 attempts, it makes sense to limit the amount of attempts so someone cannot continue trying until they finally find the right match. The two researchers do point out, however, that if the system is set to only allow a certain amount of attempts per day, a potential intruder could "mount an attack that lasts 50 days (with 20 iterations/day) and still manage to break into the account" (Uludag & Jain, 2004, p. 11). After suggesting all of their ways to help prevent attacks, Uludag and Jain (2004) state, "Even though we proposed several measures to counter such attacks, each has its own limitations, especially for multimodal biometric systems" (p. 11).

Uludag and Jain (2004) discussed the minutiae-based fingerprint scanners, but Roddy (1997) focused on the pore-based systems. These systems recognize "The uniqueness of a configuration of pores," and this "depends on several factors, such as the number of pores involved, their respective shapes and sizes, the locations of these pores with respect to each other, and so on" (p. 1391). Pores are understood to be even spaced, so "any pore in the first print matches any pore in the second print, then all pores match (neglecting

rotation effects)" (p. 1392). Roddy continues by saying, "Matching a print with this kind of distribution would be trivial," but "one must allow for the possibility of an absent sweat gland" (p. 1392). Sweat glands are where the pores form, so there could be a possibility of a space where sweat gland did not form. So how does this type of system match prints with these conditions involved? Both minutiae-based and pore-based systems use algorithms, but the pore-based systems use three criteria: position, size, and shape of the pores. Another important step of comparison for pore-based systems is actually a mixture of both types of systems. Using a minutia as a reference point can be used to "measure the position of a set of nearby pores" (p. 1394). Figure 3 shows three fingerprints being analyzed by a pore-based system.

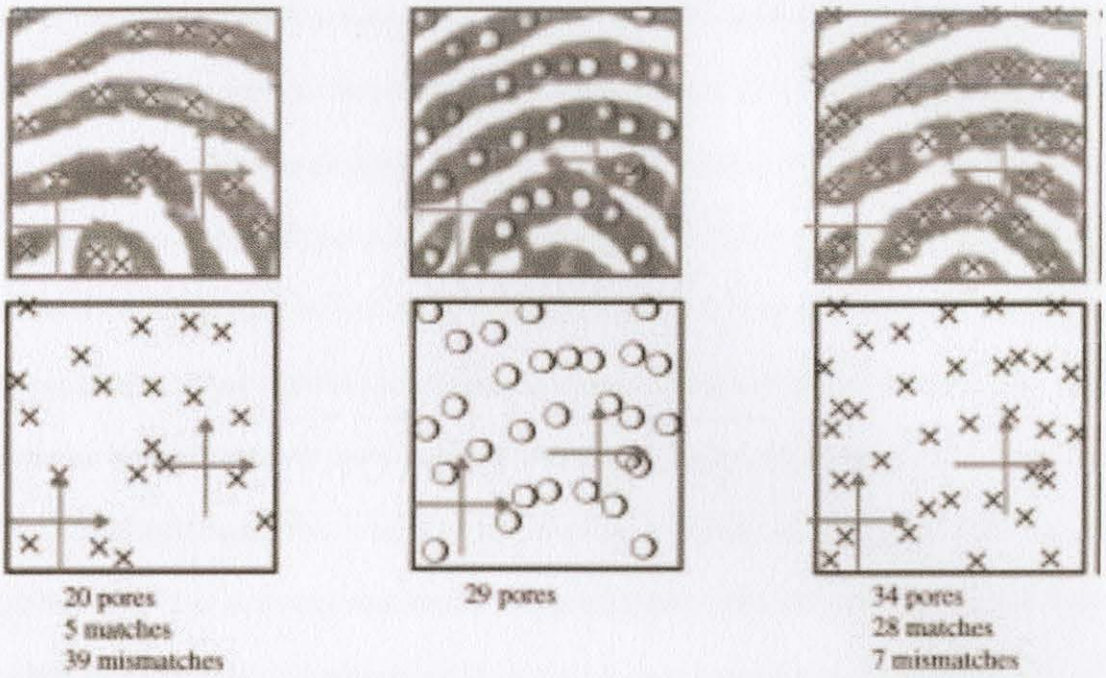

Figure 3. Examples of three prints analyzed by a pore-based system. Adapted from "Fingerprint Features – Statistical Analysis and System Performance Estimates" by Andrea Roddy, *Proceedings of the IEEE,* 1997.

Figure 3 shows pores being analyzed with and without the fingerprints' ridges. All three prints look fairly similar when you look at the ridges alone, but when the pores are analyzed it can be seen that they are very different. They also show how minutiae are used as reference points, and they all three have reference points in the same locations. Roddy (1997) states that "If the minutiae are used to align the prints, the pore information matches for the center and right images but does not match the center and left images" (p. 1396). That is because the center and right prints are actually from the same finger, so using pores can be an effective way to match a fingerprint in a database with someone trying to access a sensitive area.

Fingerprint scanners and ink have been the main way of collecting fingerprints, but new techniques are being developed to help improve this process. One of these processes that are advancing fingerprinting is 3-D Scanning. Rachel Kremen (2009)

states that "The researchers say the system is more efficient than traditional fingerprinting and significantly reduces the number of incorrect matches" (n.p.). Advances are made in many areas of science constantly, but how does this advancement affect the accepted methods of collecting fingerprints? Is it showing the flaws that are within these methods? Kremen interviewed a University of Kentucky PhD candidate graduate, Yongchang Wang. Wang stated that "Fingerprinting has been widely applied to identify criminals in forensic law enforcement and security applications" (n.p.). Wang goes on to say, "But traditional techniques don't make it easy to gather accurate, detailed points" (Kremen, 2009, n.p.). 3-D scanning requires "a series of striped lines onto a finger, in a process called structured light illumination (SLI)" (n.p.). A camera is used to take a picture of these lines so that a 3-D model of the fingerprint can be produced. Kremen claims that this method is superior in collecting prints because it does not require the finger to be rolled on a surface. This prevents the elasticity of the skin from distorting the fingerprint. The claim that this method is more efficient is a strong claim, but will it be accepted? Would more research and experimentation of this method help the field of fingerprinting see it as a step forward or a challenger to the already accepted methods of fingerprint collection?

CHAPTER VIII

HUMAN ERROR IN FINGERPRINTING

Human error can be caused by many things: lack of training, bias, and honest mistakes are only a few examples. But what if one human error could change the future of another person? That is the scenario forensic scientists deal with constantly. It has been shown in recent years that judges are becoming alarmed by the documented cases that show clear human error when dealing with fingerprints (Fisher, 2008). Fisher (2008) wrote about the Bryon Rose Case of 2006. During this case the defense argued that "the science behind fingerprint evidence has gone unchallenged, and as a result its proponents have not been forced to establish its credibility through scientific study" (n.p.). The prosecutors were shocked when Judge Susan M. Souder ruled in favor of the defense stating, "The state is correct that fingerprint evidence has been used in criminal cases for almost a century. While that fact is worthy of consideration, it does not prove reliability" (n.p.). Judge Souder went on to point out that fingerprint identification is "highly subjective" and there is a "lack of proficiency testing among fingerprint identification examiners" (Fisher, 2008, n.p.). Is there legitimacy in this ruling?

As stated before, fingerprints have been used in the criminal justice system for over a century, but more cases like the Byron Rose Case has people scratching their head about not only the process of fingerprint analysis but also the people in charge of the analysis. A great example is the Brandon Mayfield Case of 2004 (Sherrer, 2004). Brandon Mayfield was an attorney in Oregon who was accused by the FBI of bombing commuter trains in Spain. The FBI claimed they had a photocopy of a fingerprint found at the scene that matched Mayfield. This *match* was reviewed by an FBI fingerprint

supervisor and a retired FBI fingerprint examiner. The affidavit stated that "the FBI lab stands by their conclusion of a 100 percent match" (Sherrer, 2004, n.p.). There was a slight problem with the FBI's claim because Mayfield's wife stated that "we haven't been outside of the country for ten years." So was Mayfield lying or were the FBI examiners wrong in there analysis of the fingerprint found at the scene? Considering that Mayfield's print was run through AFIS and his print came up as a possible match, should that make the FBI's case even stronger? Well, in the end, the FBI was wrong. It was brought to light that twenty three days before the FBI arrested Mayfield the Spanish police notified the FBI that they believed the analysis of Mayfield's fingerprint and the fingerprint from the crime scene was "conclusively negative." It seems the FBI should have listened because later in the investigation the Spanish police found the actual source of the print to be from an Algerian man. After this, the FBI had to formally apologize to Mayfield (Sherrer, 2004). What caused the FBI to continue to pursue Mayfield as the bomber when Spanish authorities had already ruled him out? Could it have been bias? Could the two FBI examiners that reviewed the first examiner's work have assumed it was done correctly before they even had the chance to analyze the prints? It will probably never be known, but the Mayfield case is not the only case where fingerprints were analyzed wrong.

One of the most famous cases that dealt with misidentifying fingerprint matches was the Shirley McKie Case (Cole, 2005). McKie was a detective working on a homicide case with the Strathclyde Police Department in Kilmarnock, Scotland in 1997. During the crime scene investigation, a fingerprint was found in the house of the victim. The fingerprint was analyzed and the analyst concluded that the fingerprint belonged to

McKie. McKie claimed she was never in the house before the investigation, so she was charged with perjury since the fingerprint analysis clearly pointed to her. Four fingerprint examiners analyzed the fingerprints and reached the same conclusion, so the case was clearly favoring the prosecution. McKie hired two American fingerprint examiners to reexamine the fingerprints. The two American examiners claimed that "McKie could not be the source of the latent print" (Cole, 2005, p. 1010). McKie was released, but how does a mistake this large affect McKie's future? Will she ever be able to resume a normal life after all of these allegations?

The criminal justice system was dealt a hard blow when a report emerged that was made by the Los Angeles Police Department in 2008 (Rubin & Winton, 2008). The report stated that "people have been falsely implicated in crimes because the department's fingerprint experts wrongly identified them as suspects" (n.p.). Rubin and Winton share a quote from Los Angeles public defender Michael Judge showing Judge's concern of how this report could affect fingerprinting. Judge states, "This is something of extraordinary concern... Juries tend to accord the highest level of confidence to fingerprint evidence. This is the type of thing that easily could lead to innocent people being convicted" (n.p.). Considering a department exposed such a gigantic problem that plagued their entire latent print department, how can their department win back the trust and belief of the juries and judges? Could something this enormous permanently damage the reputation of the department?

Mnookin (2008) states that "Instead of offering up results from appropriately designed proficiency tests to provide a useful partial proxy for an actual error rate, fingerprint examiners have elected to fall back in court on the virtually nonsensical claim

that the technique has an error rate of zero" (p. 137). This claim of an error rate of zero has been used for decades, but considering the major cases that have had awful mistakes with the fingerprint evidence, can this assertion continue to be claimed by fingerprint experts? Again we look at what Simon Cole says about what fingerprint examiners have come to claim about the error rate. Cole (2005) says that fingerprint examiners testify that the methodological error rate of fingerprinting is zero. Does adding the word *methodological* provoke any doubt about the reliability of fingerprinting? Is saying that *the error rate is zero* not enough anymore?

Convicting an innocent person of a serious crime can ruin that person's reputation, but what happens to the reputation of a fingerprint examiner if they are responsible for that conviction? The Shirley McKie case was discussed earlier, but what happened to the analysts that made the erroneous match? McCartney (2013) reports that all of the analysts involved in the McKie case were suspended but later reinstated after one year of retraining. Even though they were reinstated, they were not allowed to appear in court as experts. McCartney says, "The fear was that the McKie misidentification would always come up and prosecutions could fail" (n.p.). This is a legitimate point, so how does a department regain the faith of the public and the courts? McCartney went on to write that the Scottish police department responsible for the misidentification of McKie created a new organization that would "retain the public confidence" (McCartney, 2013, n.p.).

Cole (2005) talks about a case in 1998 where a man named Richard Jackson was arrested for the murder of his friend, Alvin Davis. The single piece of evidence was a fingerprint found at Davis's home. Three fingerprint examiners, including a man named

Jon Creighton, came to the conclusion that Jackson was the source of the print. Knowing a mistake had been made, Jackson hired his own fingerprint examiners to analyze the fingerprint found at the scene. Both of Jackson's examiners concluded that he was not the source of the print. After both sides made their case, the jury found Jackson guilty. Knowing the jury had made a mistake, both of Jackson's examiners complained to the IAI and FBI. Both entities analyzed the evidence, and both ruled that Jackson was wrongfully convicted. Jackson was released after serving two years of prison, and the true murderer has never been arrested (Cole, 2005). Considering that the false positive the three examiners gave led to an innocent man being incarcerated for two years, was there any punishment? Cole (2005) states that Creighton, who was certified by the IAI, was decertified by the association and lost his job. The other two examiners were luckier. Neither of them lost their job or decertified. Jackson's father was outrage by this and stated, "The men who put my son away for over two years are still allowed, and have never been removed from, the ability to read prints" (Eaglin, 2009, n.p.). It is very rare for someone to go unpunished, so what usually happens when an examiners makes a mistake? This is where the *zero tolerance* policy comes into effect. German (2008) explains that "When erroneous identification decisions … are detected, most agencies immediately suspend the examiner(s) from further casework activity. German expands on the actions agencies can take. Agencies can choose different punishments, some include the following: "Return of the examiner(s) to friction ridge identification duties only after retraining and evaluation indicate the experts(s) can operate at zero identification error rate, permanent transfer to other duties, or employment termination" (German, 2008, n.p.). Examples of these measures can be seen in the previously

mentioned report that was released by the Los Angeles Police Department (Rubin & Winton, 2008). Once the errors were discovered, an internal investigation was done in the latent print department. This investigation led to the firing of one fingerprint analyst. Three analysts were suspended, and two supervisors of the unit were replaced. Rhonda Sims-Lewis, the chief of the police department's administrative and technical bureau, made this statement: "This is very, very serious. We feel very compelled to take quick action when something like this arises. Guilty people can be set free and innocent people can be jailed" (Rubin & Winton, 2008, n.p.). How many other departments around the country have problems such as these? What can be done to alleviate the problems in these departments?

Several people have argued that a big problem with fingerprint evidence is what qualifies the person on the stand to claim they are a fingerprint "expert"? The defense lawyer for Rick Jackson, Mike Malloy, stated that "The underlying problem is not the evidence itself, but is who's allowed to be qualified as an expert. The police experts were really just your local police officer, I mean, who, on a given day, might do anything from getting the cat out of the tree to examining the fingerprints" (Eaglin, 2009, n.p.). The National Institute of Standards and Technology (2012) has acknowledged that "latent print identification has been the subject of increased study, scrutiny and commentary in the legal system and in forensic science literature." Many people have called for stronger proficiency testing to keep fingerprint examiners competent and reliable in court. Ulery, Hicklin, Buscaglia, and Roberts (2011) point out that "there is no generally accepted objective measure to assess the skill of latent print examiners" (p. 7737). Mnookin (2004) states that there are proficiency tests, but the tests are "not routinely used and are

substandard" (n.p.). Mnookin also sites a claim by a fingerprint expert that the FBI proficiency tests are *absurdly easy*. If the tests themselves are called into question, what does that say about the integrity of the agency or department that uses them? Why do these different entities have their own tests that they can make however they want? That is why Mnookin calls for "systematic proficiency tests" because "they would provide significantly more information about error rates" (n.p.).

The National Institute of Standards and Technology (NIST) (2012) addressed this issue with a lengthy piece in the National Institute of Justice Journal. The NIST clearly states, "All of us make errors. This report makes no effort to hide this fact." In a field that heavily rests on the *zero error rate*, will some fingerprint examiners find this as a threat? The NIST's goal in this piece is to help lay a foundation of change that could help increase the consistency and scientific validity of fingerprinting. One suggestion made by the NIST is a "systems view of human error." They elaborate by saying, "The systems view of human error regards errors and adverse events as a function of a system of interacting parts, any or all of which could present opportunities for preventing and correcting errors" (p. 20). Considering that this system *regards errors* would this mean that the field of fingerprinting would have to admit it was wrong after decades of persistence that fingerprinting is *errorless*? How would this affect the validity of fingerprints in court? But the NIST is not pointing fingers at the fingerprint examiners. They consider fingerprinting a "complex system" and that "Simply blaming errors on individuals is simplistic and unproductive. One must appreciate how human actors function in and interact with other components of a more complex system" (p. 29). So how can a system be improved so that the examiners are less likely to commit errors?

"Well designed work environments can improve productivity, increase user satisfaction, and reduce the risk or errors and injuries" (p. 140). The NIST believes this could be something that could be corrected in fingerprinting labs because "the environment in which latent print examiners work encompasses physiological and cognitive factors; management and leadership culture, communications, and collaboration opportunities; and the physical workplace" (p. 140). Is this what went wrong in the Los Angeles Police Department (Rubin & Winton, 2008)? As mentioned before, there were numerous cases that were affected by the *poor fingerprint analysis*. The NIST mentioned *management and leadership culture*. Is this something that was missing in Los Angeles? In the report it was found that "records and evidence were left lying around or misplaced" and "people were reviewing the work of friends and just rubber stamping it without really reviewing it" (Rubin & Winton, 2008, n.p.). These are the kind of problems the NIST would like addressed. If the workplace is flawed, then the examiners are likely going to be flawed. This does not apply only to fingerprinting. The NIST wrote about an accident at a nuclear power plant. Because the control room was not designed to fit the needs of the workers, a major accident occurred. The controls were poorly placed and the instruments were not in appropriate places, so the operators could not function at their absolute best. This is when "A work environment can be disruptive, stressful, and unsafe, leading to unnecessary fatigue" (NIST, 2012, p. 142). The NIST stresses that the work environment should be designed around the fingerprint examiners so that they can function at their best and do not have to fight with the conditions in which they work. There are many problems addressed by academia and institutes such as NIST, but are they concerns that the field of fingerprinting also sees as concerns?

Human error and its causes will continue to be discussed for years to come, but how accurate are latent fingerprint examiners? Latent prints, as stated, before, are very rarely of high quality. They are usually incomplete and distorted (Triplett, 2006). An experiment was done in 2011 to test the accuracy and reliability of latent fingerprint examiners (Ulery et al., 2011). Ulery and his colleagues used "356 latents, from 165 distinct fingers from 21 people, and 484 exemplars" (p. 7734). Some of these were from "difficult comparisons resulting from searches of AFIS..." (p. 7734). Once the participating fingerprint examiners had completed their analyses, the data showed that six false positives were made out of 4.083 comparisons of nonmated pairs resulting in a false positive rate of 0.1%. Considering the *zero error rate*, this result is very close, but it is not zero. However, Ulery and his colleagues point out that none of the false positives were made by two examiners on the same comparison. They state that "Five of the six errors occurred on image pairs where a large majority of examiners made true negatives. These results indicate that blind verification should be highly effective at detecting this type of error" (p. 7738). What about false negatives? Ulery and his colleagues discovered a false negative error rate of 7.5% and that 85% of examiners had at least one false negative error. What does this mean for blind verification? Ulery and his colleagues are concerned that "verification of exclusion decisions is not generally practiced in operational procedures, and blind verification is even less frequent." This is something that can be exposed by experiments such as this and implemented into protocol for fingerprint examiners. But this study was one of many to come. Ulery and his colleagues (2011) stress that "This study is part of a larger ongoing research effort," and that this study "will assist in supporting the scientific basis of forensic fingerprint

examination" (p. 7738). Are studies such as this advancing the science of fingerprinting, or are they just revealing the vulnerability of the *zero error* claim that fingerprinting experts have been claiming for decades?

In 2001, a couple was murdered in Ireland, and the main pieces of evidence were fingerprints found at the crime scene. The defense spoke about multiple cases in the United States and the United Kingdom where fingerprints were mistakenly matched to the defendants. The detective, who was giving his testimony, Detective Sgt. Declan Buckley, spoke about his outlook on the process of fingerprint analysis. He stated, "The rate of error in fingerprint identification is zero. The rate of human error, where people do not follow the correct procedure, I am sure is higher than that, but the rate of error with fingerprint identification itself is zero" (The Irish Examiner, 2003, n.p.). What is this "correct procedure" the detective speaks of? The fingerprint examiners in Ireland do not bring fingerprints to court unless there are *12 identical characteristics* found in an analysis. Detective Buckley points out that, in the United Kingdom, fingerprint examiners do not have a set number of characteristics needed to reach a decision. Detective Buckley was asked if he had ever gotten fingerprint identification wrong, and he said no. What could be learned from this case? So many cases in recent years have questioned the validity of fingerprinting and the examiners that claim the *zero error rate*, so how can cases like this be used to endorse the legitimacy of fingerprinting?

CHAPTER IX

CONCLUSION

Over the last few decades there have been many academics and judges that have questioned the validity and reliability of using fingerprints as a method of identification. Claims have been made that there is no scientific support that fingerprints can be used as dependable evidence, but does that mean these claims are strong enough that the courts should completely ignore fingerprints? Considering that fingerprinting has been used for over a century, there may be a valid call for scientific evaluation using current methods of study. It could be easily forgotten that the time period when fingerprinting was being born had very little to work with when it comes to technology. They also did not have the resources we do today, such as AFIS and other ways of gathering data from all over the world. Even so, some of the brightest minds in the world during the 19th century spent decades studying this new idea and trying to validate fingerprinting as a means of identification. But does that mean they got it wrong since they did not have the level of technology and methods of research we have today? It may be wise to not only consider scientific evaluation but also historical evaluation when studying this topic. There have been many cases that relied solely on fingerprints found at a crime scene, and since these prints were viewed as a valid piece of evidence a criminal was taken off of the streets. The argument that fingerprint analysts should not claim with *100% certainty* that the fingerprints found at a scene match the suspect is not farfetched. Claiming that there could not be another person in the world with that print is impossible to prove considering there are over 7 billion people in the world today. But the argument could be

made that there is no way to prove that there is another person with the same fingerprint. So who wins in this argument? This is one dispute that could go unsettled.

Academics have been on the offensive for the last few decades claiming that fingerprinting is not worthy to be evidence. The academics have very intriguing arguments, and some are legitimate. Dr. Glenn Langenburg is a well-respected fingerprint analyst that pointed out some things about the academics that are attacking his field. Langenburg spoke about a professor named James Starrs who has been in agreement with Cole (2005) on many areas of fingerprinting including error rates and that fingerprinting is *falsifiable*. Langenburg said, "Starrs completed a few undergraduate science courses approximately fifty years ago. Other than that, he has no formal scientific training. He has never worked in a forensic laboratory. He does not attend crime scenes. He has not taken any formal instructional course in fingerprints. His background is English and Law" (Fingerprints East Bay, 2011, n.p.). So where does Professor Starrs draw his knowledge about the field when he has no background in it? It is like asking the question, who is the greatest basketball player of all time? Would you rather ask a sports writer who has never touched a basketball court in his life or someone who had a career playing in the NBA? The sports writer may know dozens of statistics and be able to formulate an argument, but the NBA player experienced the big and little things that go along with a basketball career and how the game is played. Even so, the academics should not be ignored. That would not be beneficial to the field of fingerprinting. It is a positive thing that people raise questions and propose ideas that could lead to a more sound and efficient method. There can be many great things taken

from the arguments of the academics such as ways to improve different processes and how to develop a better way to present fingerprint evidence in court.

Technology has come a long way in the last few decades. From the computer to the internet, the world is a more connected place than ever before. Stories can be heard from all over the world minutes after they occur. This would have taken weeks, maybe even months, only a century ago. With the addition of AFIS and other databases to the field of fingerprinting, nations have linked their databases of fingerprints with one another. Also, this database allows an analyst to input a fingerprint to see if AFIS can find a match or potential matches. This technology has been an amazing asset, but it should not be given too much power. Dr. Itiel Dror's (2012) study on the effects of AFIS on the fingerprint analyst was an eye-opener. It showed how bias can be created if the analyst begins to rely too much on AFIS. The fingerprint analysts have to remember that they have the most important role in the fingerprint evaluation process. Technology such as AFIS can be a great tool, but letting it influence your decisions can lead to careless mistakes. This could lead to an innocent person being incarcerated or a guilty person walking free.

A majority of the sources discovered during this process focused on the negative aspects of fingerprinting. It was mentioned before that fingerprints have been used for over a century to take criminals off of the streets, but some people would fire back by asking, Well what about all of the times fingerprints led to an innocent person being put in jail? The cases where this occurred can be linked by one thing: careless fingerprint analysts. The Brandon Mayfield case is a shining example of this. The FBI examiners who were in charge of the fingerprint analysis were obviously careless. The Spanish

police had already ruled out Mayfield as a suspect, so why did the FBI ignore this? Did they believe that the Spanish police were inferior when it came to dealing with fingerprint evidence? If there is a strict protocol in place for dealing with fingerprint evidence the human error rate would dramatically decline. Imagine how much more effective the Los Angeles Police Department's fingerprinting unit would have been if the analysts and supervisors would have not been so incompetent and careless. Considering the fact that evidence was allowed to pile up on desks and even misplaced numerous times shows just how poorly that unit was run. The exposure of the cases in recent years makes people question fingerprinting when they should be questioning the people involved with the analysis. Any time there is a human involved there is a chance an error may occur, but if the analyst is competent, well-trained, and careful with the examination of the evidence, fingerprinting is a reliable tool for identification. To maintain this reliability, a low tolerance for errors has been created. The *zero tolerance* rule shows that one error can lead to someone losing their job and/or certification. Once someone has this label, it is very difficult for them to get another job at the same position or get recertified. They rarely get a chance to testify in court again because the prosecution may be fearful the defense will bring up their past mistakes. When it comes to someone's life, no errors are acceptable.

REFERENCES

Barnes, J. (2011). The fingerprint sourcebook. *Scientific Working Group on Friction Ridge Analysis, Study and Technology.* Washington, DC: National Institute of Justice, 7-22

Brand, D. (2002). Fingerprint evidence – under judicial assault – unlikely to be replaced by DNA profiling for criminal identification, says Cornell researcher. *Cornell Chronicle*. Retrieved from http://news.cornell.edu/stories/2002/01/fingerprints-unlikely-be-replaced-dna-profiling

Cole, S. (2001). The Myth of Fingerprints. *The New York Times.* Retrieved from http://www.truthinjustice.org/fingerprint-myth.htm

Cole, S. (2005). More Than Zero: Accounting for Error in Latent Fingerprint Identification. *The Journal of Criminal Law and Criminology, 95*, 985-1078

Cole, S. (2009). Forensics Without Uniqueness, Conclusions Without Individualization: The New Epistemology of Forensic Identification. *Law, Probability and Risk, 8,* 233-255

Cole, S. (2009). Is Fingerprint Identification Valid? Rhetorics of Reliability in Fingerprint Proponents' Discourse. *Law & Policy, 28,* 109-135

Cole, S. (2010). Forensic Identification Evidence. *Criminology & Public Policy, 9*, 375-379

Dror, I. (2008). Meta-analytically Quantifying the Reliability and Biasability of Forensic Experts. *Journal of Forensic Science, 53,* 900-903

Dror, I., Wertheim, K., Fraser-Mackenzie, P., & Walajtys, J. (2012). The Impact of Human-Technology Cooperation and Distributed Cognition in Forensic Science:

Biasing Effects of AFIS Contextual Information on Human Experts. *Journal of Forensic Science, 57,* 343-352

Dror, I., & Mnookin, J. (2010). The Use of Technology in Human Expert Domain: Challenges and Risks Arising from the Use of Automated Fingerprint Identification Systems in Forensic Science. *Law, Probability and Risk, 9,* 47-67

Eaglin, N. (2009). Fingerprints: Infallible Evidence? *CBS News.* Retrieved from http://www.cbsnews.com/8301-18560_162-563607.html

Edwards, R. (2010). Fingerprint Identification Evidence Questioned by Senior Judge. *The Telegraph.* Retrieved from http://www.telegraph.co.uk/news/uknews/law-and-order/8144044/Fingerprint-identification-evidence-questioned-by-senior-judge.html

Ellis-Christensen, T. (2003). Can Two People Have the Same Fingerprints? *Wisegeek.* Retrieved from http://www.wisegeek.com/can-two-people-have-the-same-fingerprints.htm

Faulds, H. (1880). On the Skin-Furrows of the Hand. *Nature Magazine, 22,* 605

Ferren, L. (2010). Rare Twin Murder Case Echoes Bizarre Fingerprint Origins. *ABC News.* Retrieved from http://abcnews.go.com/TheLaw/atlanta-twin-murder-case-echoes-fingerprint-origins/story?id=9909586

Fingerprints East Bay (2011). Defending Against the Critics Curse. Retrieved from https://sites.google.com/site/fingerprintseastbay/defending-against-the-critics-curse

Fisher, J. (2008). Forensics Under Fire. *Edinboro.* Retrieved from http://jimfisher.edinboro.edu/forensics/fire/print.html

Franklin, J. (2003). What Are the Different Types of Fingerprint Patterns? *WiseGeek.* Retrieved from http://www.wisegeek.com/what-are-the-different-types-of-fingerprint-patterns.htm

German, E. (2008). Errors vs. Idents. *Onin.* Retrieved from http://onin.com/fp/problemidents.html#Zero_tolerance_explanation

Gurdoglanyan, D. (2001). Fingerprints Used in Forensic Investigations. *Bronx Science.* Retrieved from http://www.bxscience.edu/publications/forensics/articles/fingerprinting/r-fing01.htm

Haber, L., & Haber, R. (2008). Scientific Validation of Fingerprint Evidence Under Daubert. *Law, Probability and Risk*, 87-109

Inglis-Arkell, E. (2012). Your Fingerprint at the Scene of a Crime Doesn't Prove Anything. *Io9.com.* Retrieved from http://io9.com/5900223/just-how-incriminating-is-a-fingerprint-really

Inman, K., & Rudin, N. (2001) Principles and Practices of Criminalistics: The Profession of Forensic Science. Boca Raton, FL: CRC Press

The Irish Examiner. (2003). Garda Defends Fingerprint Evidence in Double Murder Trial. *The Irish Examiner.* Retrieved from http://www.clpex.com/Articles/Newz/2003/2003-02-26-2.htm

Kremen, R. (2009). Touchless 3-D Fingerprinting: A new system offers better speed and accuracy. *MIT Technology Review.* Retrieved from http://www.technologyreview.com/news/415513/touchless-3-d-fingerprinting/

Lawson, T. (2006). Can Fingerprints Lie?: Re-weighing Fingerprint Evidence In Criminal Jury Trials. *Journal of Criminal Law, 31,* 1-66

Leadbetter, M. (2005). Fingerprint Evidence in England and Wales – The Revised Standard. *Medicine, Science, and Law, 45,* 1-6

McCartney, C. (2013). Flawed Fingerprint Expert Won't Be Getting Job Back. *Wrongful Convictions.* Retrieved from http://wrongfulconvictionsblog.org/2013/01/26/flawed-fingerprint-expert-wont-be-getting-job-back/

Mears, M. (2003). The Challenge of Fingerprint Comparison Opinions in the Defense of a Criminally Charged Client. *Georgia State University Law Review, 19,* 1-56

Mnookin, J. (2004). A Blow to the Credibility of Fingerprint Evidence. *The Boston Globe*. Retrieved from http://www.boston.com/news/globe/editorial_opinion/oped/articles/2004/02/02/a_blow_to_the_credibility_of_fingerprint_evidence/

Mnookin, J. (2008). The Validity of Latent Fingerprint Identification: Confessions of a Fingerprinting Moderate. *Law, Probability and Risk, 8,* 127-141

National Institute of Standards and Technology. (2012). Latent Print Examination and Human Factors: Improving the Practice Through a Systems Approach. *National Institute of Justice Journal, 270,* 6-254

Pankanti, S. (2002). On the Individuality of Fingerprints. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 24,* 1010-1025

Peterson, P., Dreyfus, C., Gische, M., Hollars, M., Roberts, M., Ruth, R., Webster, H., & Soltis, G. (2009). Latent Prints: A Perspective on the Slate of the Science. *Forensic Science Communication, 11*

Prabhakar, S. (2002). Learning Fingerprint Minutiae Location and Type. *Pattern Recognition, 36,* 1847-1857

Richard McCoy vs. State of Florida (2013). No. SC10-2206, 1-45

Roddy, A. (1997). Fingerprint Features – Statistical Analysis and System Performance Estimates. *Proceedings of the IEEE, 85,* 1390-1421

Rubin, J., & Winton, R. (2008). LAPD Finds Faulty Fingerprint Work. *Los Angeles Times.* Retrieved from http://articles.latimes.com/2008/oct/17/local/me-fingerprints17

Russell, S. (2012). Why Fingerprints Aren't the Proof We Thought They Were. *Pacific Standard.* Retrieved from http://www.psmag.com/legal-affairs/why-fingerprints-arent-proof-47079/

Salter, D. Fingerprinting – an Emerging Technology. *New Mexico State University.* Retrieved from http://technologyinterface.nmsu.edu/summer97/security/finger.html

Sherrer, H. (2004). That's Not My Fingerprint, Your Honor. *Justice: Denied, 25,* 11-14

Spinney, L. (2010). The Fine Print. *Nature, 464,* 344-346

Sumayao, M. (2003). How do Police Gather Latent Fingerprints? *WiseGeek.* Retrieved from http://www.wisegeek.com/how-do-police-gather-latent-fingerprints.htm

Thornhill, T. (2011). Spot the Difference? The strange case of the criminal doppelgangers that sparked the need for fingerprinting. *Mail Online.* Retrieved

from http://www.dailymail.co.uk/news/article-1392418/The-amazing-pictures-sparked-need-fingerprinting.html

Tredoux, G. (2003). Henry Faulds: the Invention of a Fingerprinter. Retrieved from http://galton.org/fingerprints/faulds.htm

Triplett, M. (2006). The Etiology of ACE-V and its Proper Use: An Exploration of the Relationship Between ACE-V and the Scientific Method of Hypothesis Testing. *Journal of Forensic Identification, 56,* 345-355

Ulery, B., Hicklin, A., Buscaglia, J., & Roberts, M. (2011). Accuracy and Reliability of Forensic Latent Fingerprint Decisions. *Proceedings of the National Academy of Sciences of the United States of America, 108,* 7733-7738

Uludag, U., & Jain, A. (2004). Attacks on Biometric Systems: A Case Study in Fingerprints. *Michigan State University,* 1-12

Wise, J. (2004). Under the Microscope: Legal Challenges to Fingerprints and DNA as Methods of Forensic Identification. *International Review of Law Computers & Technology, 18,* 425-434

Zonana, H. (1994). Daubert V. Merrell Dow Pharmaceuticals: A New Standard for Scientific Evidence in the Courts? *Bull Am Acad Psychiatry Law, 22,* 309-325