NOTE: The following article:

Fingerprints, by Melissa Stewart

Were scanned from American Heritage of Invention and Technology, Volume 17, No.1, Summer 2001.

This article is copyrighted 2001 by American Heritage, An affiliate of Forbes Inc., 90 fifth Avenue, New York, NY 10011.

This article is included to provide an introduction to forensic science for educators and students under the fair use provisions of copyright law as educational information.
NATURE GAVE EVERYONE AN INFALLIBLE PROOF OF IDENTITY EVEN BEFORE DNA.
Fingerprints

SINCE ANCIENT TIMES, fingerprints have been recognized as a definitive means of establishing who someone is. Unlike faces, handwriting, or other characteristics, they are unique to each person and cannot be imitated. They do not change over time, and despite the attempts of criminals to efface their prints with sandpaper, acid, or surgery, they cannot be disguised or permanently altered.

Evidence exists of their use among the prehistoric residents of Nova Scotia. In ancient China and Egypt, criminals had their fingerprints recorded for future reference, while, in Babylon, fingerprints sealed business transactions. Other civilizations that have used fingerprints include those of ancient Assyria and Japan and medieval Peru and Persia.

In 1686 Marcello Malpighi, a professor of anatomy at the University of Bologna, wrote the earliest scientific treatise on fingerprints. A more detailed discussion, with the first rudimentary attempt to classify different patterns, was published in 1823 by John Evangelist Purkinje of the University of Breslau, in Prussia. It attracted little notice. Not until the late nineteenth century did fingerprints begin to be used systematically for identifying individuals and solving crimes. As with other technologies, fingerprinting could not achieve its potential until information about it was widely disseminated and a critical mass of users developed.

Those conditions began to be satisfied in 1880, when Henry Faulds, a Scottish physician living in Tokyo, published the first modern inquiry into the variety and uniqueness
of fingerprints. In the October 28 issue of *Nature*, Faulds described different types of prints, noted that they remain constant through an individual's life span, and suggested that "when bloody finger marks or impressions on clay, glass, etc., exist, they may lead to the scientific identification of criminals."

Faulds's work was not purely theoretical, for he had concrete proof that fingerprinting could be used to catch and convict wrongdoers. In his years of collecting fingerprints as a hobby, he had taken impressions from most of the people who lived in his neighborhood. When a nearby house was robbed, he decided to conduct his own investigation.

He compared the fingerprints he found on a teacup with his recorded prints of the people who lived in the house and found no matches. This excited Faulds. Maybe the prints on the cup belonged to the thief. He spent hours poring over his extensive collection until he found a match. It belonged to a servant from a neighboring household. When the police called the servant in for questioning, he confessed. This case made Faulds the first person on record to solve a crime using fingerprints.

Like DNA evidence, fingerprints could also save an innocent person from jail. During another burglary, the thief left his sooty fingerprints on a whitewashed wall. When Faulds heard that the police had a suspect in custody, he got their permission to take the man's fingerprints. They didn't match the ones from the wall, and Faulds persuaded the police to release the man. A few days later, another suspect was arrested. His prints were identical to the sooty set on the wall, and he was later convicted of the crime.

It turned out that Faulds was not the only person doing research on fingerprints. Four weeks after his article appeared in *Nature*, the same journal published a letter from Sir William James Herschel, the grandson of a prominent astronomer, who was an official with the British colonial government in Bengal, India. One of his duties was overseeing the issuance of pension checks to retired soldiers, most of whom were Indian. Many of the pensioners were illiterate or could not write their names in English. They signed for their pensions with an X, which made it easy for an impostor to fraudulently obtain someone else's check. Without photographs or any other type of identification, these impostors were nearly impossible to catch.

Herschel responded to the problem with a simple and effective solution. There was nothing new about Faulds's discovery of fingerprinting, he wrote to *Nature*, for "I have been taking sign-manuals [i.e., signatures] by means of finger-marks for now more than twenty years." Herschel also fingerprinted convicted criminals. With their prints on file, convicts could no longer obtain leniency by claiming that they had never been imprisoned before, nor could they pay someone to serve a jail sentence for them. Fingerprints came to be used for identification in a number of government functions in India, including as a receipt for payments to opium growers.

Reports of Faulds's article and Herschel's response caught the attention of people in literary and scientific circles. Mark Twain made fingerprint identification of a murderer a central plot point in *Pudd'nhead Wilson*, published in 1894. Even then, Twain could be confident that few of his readers would be familiar with fingerprinting, for it was still employed only rarely and haphazardly. The first recorded use of fingerprints for identification in the United States had come in 1882 in New Mexico, when Gilbert Thompson, a topographer with the U.S. Geological Survey, used his fingerprint to authenticate official documents. Around the same time, fingerprints were suggested as a means of registering Chinese immigrants.

Neither Faulds nor Herschel nor any of their predecessors had taken the next step: finding a systematic way to classify and search through a large assemblage of prints. No such system had been necessary to use fingerprints for verification (a yes-or-no check of someone's identity) or selection (comparing a print with those from a small group of suspects). But to perform identification (a full-scale search through an archive) on anything other than a needle-in-a-haystack basis would require some sort of filing system.

The system in place in most of the world today was set forth in 1896 by Edward R. Henry, a British police official stationed in India. Henry had been interested in fingerprints for a long time. Two years earlier, while in England on vacation, he had visited the distinguished scientist Francis Galton. Galton was a wealthy polymath who had made valuable contributions in medicine, physiology, African exploration, meteorology, scientific instrumentation, statistics (though an untrained amateur, he laid critical groundwork for the concepts of correlation coefficients and regression analysis), psychology, and eugenics.

His studies in the last of these fields, inspired in part by the work of his cousin Charles Darwin, led him to record body measurements and other information for large numbers of people in order to sift through the results for patterns. Along the way—in addition to compiling, in the words of a biographer, "a map to show the geographical distribution of beauty in Great Britain"—Galton got interested in fingerprints. His curiosity had been piqued by the publications of Faulds and Her-
schel, and the latter sent him a huge package of material. After examining it, Galton decided to collect his own data and proceeded to fingerprint everyone who visited him.

Over the next few years he devoted a great deal of time and energy to analyzing and applying the results. In 1892 he published a book on the subject, followed by others in 1893 and 1895. He made no claim of originality, writing that "finger-prints have been proposed over and over again before now as a means of identification." Instead, he described a primitive system for classifying prints, admitting that it would need more work to become useful. He also described the "minutiae"—forks, dots, islands, hooks, and bridges—that make each fingerprint unique. These features are sometimes known as "Galton's details."

Just as Faulds and Herschel had inspired him, so Galton in turn captured the imagination of Edward Henry, who began to mull over the problem of classification. One day in 1895, as Henry was taking a train to Calcutta, an idea struck him. He pulled a pencil from his pocket, and, having no paper, he began to sketch out his ideas on the sleeves of his crisp white shirt. Before long his sleeves were covered with a slew of formulas.

Those formulas yielded the famous Henry system, which, with a few modifications, is still employed today by hospitals, hotels, banks, government agencies, and police departments in most of the world. Spanish-speaking countries are the chief exception; they tend to favor a different system, developed around the same time as Henry's by Juan Vucitch of Argentina. Vucitch was an ardent promoter of his system, and early in the twentieth century, at his urging, Argentina's government instituted mandatory universal fingerprinting. Many years later that policy proved tragically useful for identifying the remains of victims who had been "disappeared" by the state security apparatus during the 1970s.

Henry's system was based on the three basic types of fingerprint patterns: loops, which consist of ridges that begin and end on the same side of the finger; arches, which begin and end on opposite sides; and whorls, which have a spiral or bull's-eye shape. (The small fraction of prints that do not fall into any of these categories are known as accidentals.) Loops can be subdivided into radial and ulnar varieties, which incline toward the thumb and the little finger, respectively. Arches, similarly, can be divided into plain (a modest rise) and tented (a sharp peak). About 65 percent of all fingerprints are loops, 30 percent whorls, and 5 percent arches.

Once the basic type has been established, further identification is done by counting the ridges in between features known as deltas and cores. A typical Henry code might look something like 132 27 6 14, with some of the numbers and letters denoting the presence or absence of whirls on certain fingers, while others indicate the number of ridges in particular places.

The Henry system gives a unique code to each person, not to each fingerprint. It was designed for use when a complete set of prints has been taken—from a criminal in custody, for example, or an applicant for a government job—in order to find out quickly if the archives contain a matching set. When no complete set is available, as when a single print is taken at a crime scene, the Henry system is less useful.

For this reason, law-enforcement bureaus maintain separate "single print" files for career criminals, usually subdivided by the type of crime a subject specializes in. These are based on a system invented in 1930 by Harry Battley and Frederick Cherrill of Scotland Yard. If a single print was left at a crime scene

Above: The Bertillon system classified body parts, such as ears. Right: A New York City policeman sizes up a perp around 1900.
by a known lawbreaker, it can be found in these files fairly easily. If it was left by someone else, investigators may have to search through hundreds or thousands of cards to find a match—a task that was often hopeless before computerization.

In June 1897, under Henry's supervision, the world's first fingerprint bureau opened in Calcutta. Soon an opportunity to test it arose. In August 1898, the manager of a tea plantation was brutally murdered in his home. The police had very little evidence to go on besides a fingerprint the culprit had left on a card in the victim's wallet. Henry asked the local police to send him the card. He also asked for the fingerprints of the dead man, his family, and everyone who worked for him.

When Henry found no matches, he painstakingly combed through the thousands of fingerprint records on file in his office, using his classification system as a rough guide to narrow the search. Henry knew he would find the prints on file only if the murderer had previously been arrested. Fortunately, after weeks of searching, he found a perfect match. It belonged to a former servant on the plantation who had been convicted of theft two years earlier. The servant, named Charan, was arrested, tried, and convicted of murder largely on the basis of Henry's fingerprint evidence, which the court accepted as scientifically sound.

News of the Charan affair spread quickly, as British newspapers picked up the story. Detectives at London's Scotland Yard heard about Henry, and in 1901 he got a new job: assistant police commissioner and head of the Criminal Investigation Department at Scotland Yard. Henry immediately put his system to work in Great Britain. Soon afterward, it was brought to the United States.

A fingerprinting exhibit by British experts at the 1904 world's fair in St. Louis contributed to the spread of fingerprinting in the United States. The St. Louis police were so impressed that they became the first American department to officially adopt the Henry system for solving crimes. Rival systems, such as one invented by James H. Parke of the New York State Prison Department, also achieved some popularity, but as time went by, the Henry system came to be all but universal in the United States.

Police departments from Boston to San Francisco took it up with varying degrees of enthusiasm, depending on how receptive the chief was to new ideas. Elsewhere, the Navy fingerprinted recruits to keep them from deserting and re-enlisting under other names, and in an echo of Herschel's original procedure, the government used fingerprints on reservations as a way for American Indians to execute documents.

Perhaps the most tireless advocate of fingerprinting was Joseph A. Faurot, a detective in New York City's police department. In the face of indifference from his superiors, he scored a coup by using fingerprint evidence to identify a notorious international hotel burglar in 1906 and a murderer who had beaten a woman to death in 1908. Yet, while fingerprints were proving their value to police, they were little help to prosecutors, since no American judge had seen fit to admit fingerprint evidence at a trial (the criminals apprehended by Faurot had all confessed).

The shaky legal status of fingerprinting ended in 1911, when a Chicago man named Thomas Jennings was tried for
breaking and entering and murder. Jennings denied any involvement in the crime, but his fingerprints matched four that had been recovered from the murder site. (By chance, a railing next to the window through which Jennings had entered had been painted just hours before, and the fresh paint had preserved Jennings's prints.) These prints were admitted into evidence and formed the basis of the prosecution's case. Jennings was convicted and sentenced to death, and on December 21, 1911, the Illinois Supreme Court upheld the conviction.

"When photography was first introduced," the Illinois justices wrote, "it was seriously questioned whether pictures thus created could properly be introduced in evidence, but this method of proof, as well as by means of X-rays and the microscope, is now admitted without question... why does not this record justify the admission of this fingerprint testimony under common law rules of evidence?"

Shortly afterward, a dramatic courtroom demonstration further boosted the legal use of fingerprints. In New York City, Faurot had identified a loot burglar by means of fingerprints, and when the burglar refused to confess, his case went to trial. When the prosecutor tried to introduce Faurot's fingerprint evidence, a skeptical judge decided to perform a test. After sending Faurot into his chambers, the judge selected 15 people from the courtroom and asked them to put their fingerprints on a windowpane. Then he chose one of them to put a second print on another piece of glass. Faurot was brought back to the courtroom, and the judge challenged him to determine which of the 15 prints on the window matched the print on the glass. Faurot identified it within half an hour. Following this proof of the power of fingerprinting, the defendant was found guilty. Higher courts sustained the conviction.

With these highly visible triumphs, fingerprinting came to be universally accepted. Soon every police department of any size was taking prints, as were prisons, the military, and oth-
er organizations. Law-enforcement officials realized that this large volume of records would be an invaluable national resource if it could be made accessible to those who needed it. Toward this goal, Congress in 1924 established the Identification Division of the Federal Bureau of Investigation. It was headed by a young Department of Justice employee named J. Edgar Hoover and staffed by trained experts (unlike the archive at Leavenworth, where a reliance on convict labor tended to compromise the integrity of the records). At its inauguration, the FBI archive had about 810,000 fingerprint cards on file.

The FBI began a series of nationwide efforts to fingerprint as many people as possible, with schools, youth groups, and fraternal organizations all joining in. These campaigns attracted broad public backing, though civil libertarians objected. One selling point was that fingerprints could be used to identify disaster victims, lost children, missing persons, and amnesiacs, but Roger Baldwin of the American Civil Liberties Union pointed out that very few people would ever fall into any of these categories. He also asserted, less supportably, that fingerprints would be little help in law enforcement because criminals could simply wear gloves. Instead, he saw fingerprinting as the first step in a nationwide system of snooping and government control.

As early as 1925, The American Mercury had pointed out that fingerprints could be lifted from one surface and duplicated on another. The publication warned that corrupt police might be able to frame innocent suspects in this way. A decade later, under the heading “Fingerprints of Fascism,” an editorial in The New Republic decried a Berkeley, California, fingerprinting campaign, arguing with questionable accuracy that “very few of the country’s leading criminologists share the enthusiasm of California’s eager amateurs as to the effectiveness of fingerprinting as a crime preventive.” It went on to say that “there seems no doubt that the instigators of the Berkeley fingerprinting jamboree are in fact people with strong fascist leanings.” (In proof of this assertion, the editors cited the participation of the California Junior Chamber of Commerce.)

As understanding of fingerprinting spread among police, numerous ways were found to bring out “lattents”—prints that are not visible to the naked eye. The most common method was, and remains, dusting, which is familiar to fans of television crime dramas. In this procedure, a fine powder—which may contain graphite, resin, lampblack, mercury, or aluminum mixed with chalk—is sprinkled on a soft-haired brush and gently dusted over areas where prints might be. The powder, generally dark for use on light surfaces and vice versa, sticks to the fingerprint lines, which consist of sweat and oil discharged from pores on the fingers’ ridges.

Dusting works best with prints left on hard, smooth substances, such as glass, metal, or plastic. But researchers have devised more than 40 ways to develop latents, including the use of silver nitrate, iodine, ninhydrin, gentian violet, fumes of cyanoacrylate (an epoxide-like substance), and even lasers, which can make fingerprints glow in the dark. Each method has a particular situation and type of surface in which it works best. The more complicated and expensive procedures are reserved for major crimes.

Over the years, a steady stream of articles and encyclopedia entries, sometimes written by Hoover himself, reported with implausible precision the growth of the FBI’s collection: 6,398,359 sets of prints in October 1936; 130,460,252 in April 1954; 146,126,059 in August 1957 (though, as Hoover pointed out, “it is estimated that these cards represented 73,482,892 individuals”). As this and other collections of fingerprints grew, so did the task of managing and organizing them. Since the 1930s, holes punched in the edges of record cards had allowed them to be searched and sorted with data-processing machinery. The beginnings of modern computer-based fingerprint identification can be traced to 1967, when the FBI started developing scanning equipment to read and record fingerprint minutiae. A prototype was up and running by 1972.

The agency then began creating a computerized database with fingerprint records and descriptions of all first-time offenders. By 1979 it was possible to search the database by name or by various sorts of descriptive data. In the mid-1980s, police departments in most large cities adopted similar systems. Such databases can be searched now for sets of ten prints, for features found in incomplete prints, and more. The fastest of them can examine more than 1,000 prints per second.
The results of computerization were astounding. In 1978 a 48-year-old woman was murdered in San Francisco. Police recovered several fingerprints from the crime scene and spent countless hours searching through at least 300,000 fingerprint records. Despite their monumental effort, they never found a match. Then, in 1985, a computer search identified the murderer in six minutes. First the prints taken at the crime scene were scanned in and compared with the digital archive; then the computer printed out a list of possible matches, which an officer examined visually to find one that corresponded exactly. A suspect was arrested and pleaded guilty to first-degree murder.

That same year, in Los Angeles, the horrific Nightstalker was identified on the basis of a partial fingerprint he had left in a stolen car. Such a clue would normally have turned out to be no more than tantalizing, since the killer was not in the police department's file of known criminals (the turned out to be a drifter who had been arrested only on a minor traffic infraction). But just months before, Los Angeles had installed a computerized fingerprinting system, which found a match in minutes. The killer's name and photograph were released to the media, and he was captured a few days later.

In the mid-1990s, the FBI computerized its entire archive by scanning in all its old paper records. (Today, electronic finger scanning eliminates the paper stage entirely, as a laser beam scans a fingerprint electronically and stores its characteristics in electronic form.) The bureau also connected itself with major police departments in a nationwide network, allowing participants to exchange fingerprint records electronically.

The project was completed in 1999, and today local police can take someone into custody, send his or her fingerprints to the FBI, and find out in as little as two hours if the suspect has a criminal history or is wanted in connection with a crime. In the past, this process often took 10 weeks or more. Every month, fingerprint matches help apprehend more than 2,700 fugitives in the United States.

As in the 1920s and 1930s, fingerprinting is not without its critics. The legal scholar Simon Cole points out that while all sorts of technology may be used to store and retrieve fingerprints, when two of them are compared, the final match-or-no-match decision is still made by eyeballing. No definitive standard exists for deciding if a pair of fingerprints, which may have been taken at different times with different methods, are identical. Some examiners require a certain number of points of similarity, while others shun formal guidelines and rely on an overall impression.

The absence of a uniform standard, says Cole, leaves too much room for interpretation, making it possible for fingerprints that may differ slightly to be identified as the same. This problem is particularly troublesome when suspects are identified on the basis of smudged or partial prints. Some criminal defense lawyers assert that fingerprint identification, as currently practiced, does not meet the Supreme Court's standards for admitting scientific evidence at trials.

Today's finger-scanning technology has applications far beyond law enforcement. For example, scanners can be used to control who is allowed into military facilities and out of prisons, to limit access to computer networks and patient files at

**EVERY MONTH, COMPUTERIZED FINGERPRINT MATCHES HELP**

**APPREHEND MORE THAN 2,700 FUGITIVES IN THE UNITED STATES.**

Left: A 1937 photograph shows how dusting can reveal latent prints. Above: Taking a fingerprint from a gun with red dye.
In recent years palm prints have increasingly been used for identification.

not make sense to install a finger scanner in a setting where people are likely to have dirty hands. Moreover, about 2 percent of the population do not have recordable fingerprints. In 1996 Push Grover, a native of India who had lived in the United States since 1970, decided to apply for U.S. citizenship. Anyone seeking citizenship is required to provide a set of fingerprints that can be checked against the FBI’s files. Grover had tried 11 times at last report, but she had not been able to provide a set of prints; only black smudges appeared. Her fingers simply lacked the ridges that make up normal fingerprints.

Lawton Chiles, the former governor of Florida, is another example. In 1995 his state began a voluntary program to let drivers have their fingers scanned to prevent their licenses from being renewed or replaced fraudulently. The governor decided to publicize the program by becoming the first enrollee, but when he pressed his thumb on the scanner, nothing happened. In an effort to save the day, an aide volunteered to take the governor’s place. The device could not record her fingerprint either. When the pilot program ended, the state decided to stop using the finger-scanning device.

Because of these and other limitations, companies are working on other biometric devices that store and compare unique, measurable biological traits. Modern biometric tools are available to scan hands, retinas, and irises and to recognize faces, voices, and signatures. Products now in development will evaluate body odor and a person's gait. Meanwhile, for forensic purposes, DNA evidence is quickly coming to be seen as definitive.

Biometrics is a flourishing business. According to the International Biometric Group, an industry association, approximately $260 million was spent on biometric devices in 1999. More of this money was spent on finger scanning than on any other type of technology. About two-thirds of all companies manufacturing biometric equipment focus their attention on finger-scanning systems. As the technology improves and sales increase, systems will get less expensive. In 1994 the smallest finger scanner was the size of a desk telephone and cost $2,000. Five years later a scanner that could do the same job was the size of two sugar cubes and cost just $99. In 2003 the same device will probably sell for about $15.

The potential for biometric devices to become nearly ubiquitous has implications that certain observers find troubling. What some people call security, others call repression, and what some people call identification, others call invasion of privacy. Like photography, sound recording, and many other technologies, biometrics can be made to serve good or bad ends. Public awareness and understanding of biometrics will be the best way to ensure that the future is closer to Mark Twain’s Pudd’nhead Wilson than to George Orwell’s 1984.

MELISSA STEWART is a freelance writer in Marlborough, Massachusetts.
RECORDING A SET OF FINGERPRINTS, as seen here in a mid-century photograph, is just the first step. To be useful, they must then be classified, filed, searched, and retrieved when needed. To find out how technology has applied nature's built-in proof of identity, see page 22.

BETTMANN/CORBIS