Fingerprint Matching Techniques Need Reform

January 22 2007

Fingerprint matches -- key to fighting international terrorism and keeping criminals off the street -- are no longer foolproof, warns a law professor at the University of California, Davis.

Professor Edward Imwinkelried, one of the nation's leading experts on scientific evidence, and co-author Mike Cherry, who designs identification systems, say the reliability of fingerprint identification has declined while the population of the world -- and its fingerprints -- has exploded.

"We can no longer naively assume the reliability of our current fingerprint standards," they write in "How We Can Improve the Reliability of Fingerprint Identification," an article recently published in Judicature. "Given the stakes -- not only justice in a particular case but national security itself -- we must do better."

Imwinkelried, the Edward Barrett Jr. Professor of Law at UC Davis, and Cherry, who is vice chair of the digital technology committee of the National Association of Criminal Defense Lawyers, urge reforms.

The current matching process identifies ridges within a fingerprint and categorizes it into one of three general patterns -- including loops, arches and whorls -- and their subpatterns, and maps predetermined shapes and contours. A fingerprint is said to match when the pattern, subpattern and some of the shapes and contours roughly correspond with each other.

Population and digitization

In the late 1800s, Sir Francis Galton developed the first system for classifying and identifying fingerprints. He is quoted as having famously said that the odds of two individual fingerprints being the same are one in 64 billion. The authors point out that the current world population exceeds six billion persons, and most have 10 prints. In short, they say, the world population of fingerprints now exceeds the odds Galton estimated.

At the same time, the authors say, fingerprint matching techniques that once used cards and then analog photographs to compare up to 10 fingerprints have been taken over by automated computerized systems that use less precise digital images and pre-screen matchers that sometimes use only a single index finger.

"If we're going to rely on the computer technology for the Watch List on terrorism, when we do background checks ... we've got to have some assurance the computer system is reliably accurate," said Imwinkelried. He is co-author of "Scientific Evidence," one of the leading treatises in its field that has been cited on several occasions by the U.S. Supreme Court.

Call for new matching criteria

Imwinkelried and Cherry call for high-powered computer analysis of existing fingerprint databases -- data mining -- to detect new patterns and develop new criteria for matching fingerprints. And they urge the return to the Henry Fingerprint Classification System, which used all 10 fingers to classify an individual.

The Henry system, Imwinkelried and Cherry say, would better help

identify suspects who use aliases and would prevent criminal suspects like alleged serial killer Jeremy Jones from being re-released after each arrest because just one print is used for matching.

"If analyzed properly, fingerprints can be as accurate as DNA," they say.

In an earlier Judicature article, Cherry and Imwinkelried argue for greater skepticism of the use of computerized fingerprint analysis, especially for its reliance on digitized images of fingerprint patterns. "The bottom-line is that digital images are simple, incomplete approximations of the images they attempt to capture," they write.

The two authors call on courts to take a more skeptical look at fingerprint testimony, recommend that computer systems check as many fingerprints as are available, and advise greater scrutiny of the matching criteria embedded in the programs that match fingerprints.

Source: University of California, Davis