Posted 10/18/19

TECHNOLOGY'S GREAT – UNTIL IT'S NOT

Police love Rapid DNA and facial recognition but hate encryption. Privacy advocates beg to differ.

By Julius (Jay) Wachtel. DNA's forensic applications date back to 1984, when Dr. Alec Jeffries discovered that he could distinguish between family members by comparing repeat sequences of linked chemical pairs in their genetic code. Within a couple of years he used the technique to assist police, and in the process helped free an unjustly accused man. DNA's usefulness for fighting crime (and exonerating the innocent) quickly became evident, and its use took off.

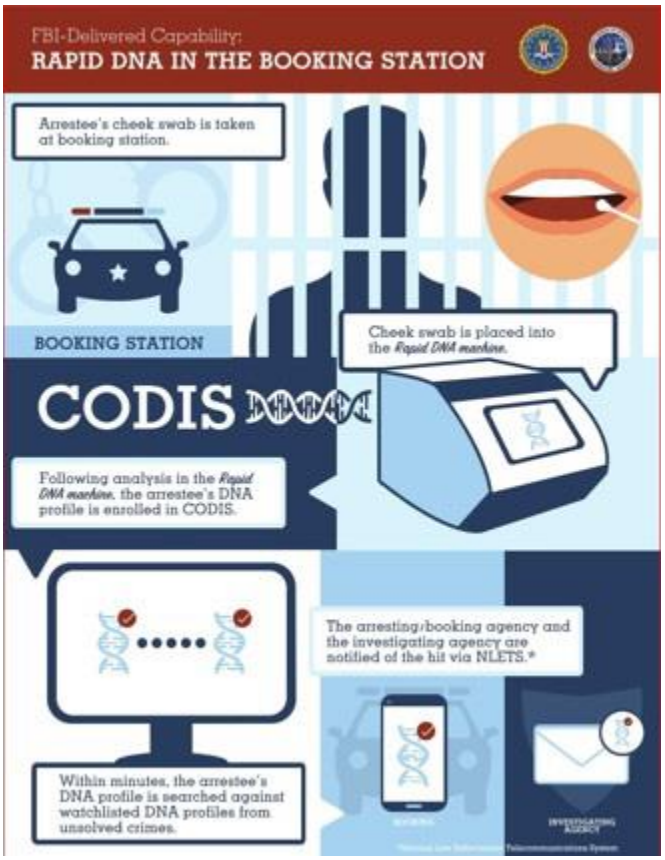
Forensic DNA analysis is couched in probabilities. An absolutely positive match, with the likelihood of error less than one over the population of the Earth, requires that samples have identical linked pairs at each of thirteen standard locations ("loci") in the human genome. (For more on this see our interview with a real expert at "DNA: Proceed With Caution.") Attaining that level of certainty is not difficult when DNA is abundant, say, from a cheek swab. But things can get tricky with crime scene evidence, and especially when the DNA is a mix with multiple contributors.

Processing DNA involves four steps: extracting whatever DNA may be present; measuring its quantity and assessing its quality; using the "PCR" method to make millions of copies of DNA sequences; and finally, separating the DNA molecules, reducing their characteristics to a profile that can be compared with other samples. Each step involves different groups of highly-skilled technicians laboring in clean rooms using specialized tools and expensive machines. Even under the most favorable conditions,

and with the most up-to-date equipment, traditional DNA typing can consume an entire day.

That's why the notorious backlog. Despite an infusion of local, state and Federal funding, the reported "average" wait for results is – hold on! – *five months*. (For information about the Fed's DNA "backlog reduction program" click here.)

Now imagine a lone operator doing it all in less than two hours with a single machine! That's what "Rapid DNA" is all about. First used in criminal casework by the Palm Bay, Florida police department, Rapid DNA has been adopted by many local and state agencies, most recently the Kentucky State Police. So far, though, the newfangled machines work best with substantial quantities of single-source DNA (i.e., cheek swabs) and tend to be flummoxed by small or mixed samples, such as "unknown" DNA found at crime scenes. Accordingly, Rapid DNA profiles are not considered sufficiently trustworthy for inclusion in or comparison with the approximately eighteen million DNA profiles of local, state and Federal arrestees and convicted persons present in the FBI's national CODIS database, which were processed in the old-fashioned, time-consuming way.



However, a major Federal initiative is underway to upgrade Rapid DNA technology so that its output is acceptable for CODIS. If it succeeds, and DNA typing becomes, as the FBI's "infographic" tantalizingly suggests, a routine aspect of the booking process, police could quickly compare crime scene DNA with genetic profiles of most anyone who's run seriously afoul of the law. And yes, its use to that end has been endorsed by the "Supremes." Here's what our nation's highest court said in *Maryland v. King* (2013):

When officers make an arrest supported by probable cause to hold for a serious offense and bring the suspect to the station to be detained in custody, taking and analyzing a cheek swab of the arrestee's DNA is, like fingerprinting

> and photographing, a legitimate police booking procedure that is reasonable under the Fourth Amendment.

At present, U.S. Government agencies collect DNA "from individuals who are arrested, facing charges, or convicted, and from non-United States persons who are detained under the authority of the United States, subject to certain limitations and exceptions" and "to preserve biological evidence in federal criminal cases in which defendants are under sentences of imprisonment." Each State also permits or requires collecting DNA from persons convicted of felonies, and thirty authorize it for certain classes of arrested persons. California, for example, allows DNA typing of everyone arrested for a felony and of a misdemeanor should they have a prior felony conviction.

Although there have been problems with DNA technology, and the legal authority to collect it is occasionally challenged, even the staunchest civil libertarians will concede that when it comes to wrongful arrest and conviction DNA has been an overwhelming force for good. But the advent of Rapid DNA – read, "cheap and quick" – has enabled the technique's use in politically controversial areas.

Such as immigration enforcement. DHS, for example, recently deployed Rapid DNA at the Southern border to combat fraudulent claims by would-be immigrants that the children who accompany them are blood relatives. Its successful use to confirm parentage inspired a Federal initiative that would collect DNA from everyone in immigration custody and transmit it to CODIS. That goal, which was clearly unattainable until Rapid DNA came on scene, was first authorized by a 2008 Federal rule that sought to use DNA "to solve and hold [unauthorized immigrants] accountable for any crimes committed in the United States…before the individual's removal from the United States places him or her beyond the ready reach of the United States justice system." But the ACLU balked. Here's what one of its lawyers said:

> That kind of mass collection alters the purpose of DNA collection from one of criminal investigation basically to population surveillance, which is basically contrary to our basic notions of a free, trusting, autonomous society.

Similar concerns have been voiced about the emerging field of facial recognition. Unlike DNA, the technology used to identify persons from photographs and video images isn't sufficiently trustworthy to use in court. Instead, it's all about generating investigative leads. Thanks to artificial intelligence software, detectives with, say, a robbery video can quickly scour photo databanks – think passports, driver licenses,

criminal record repositories, online social networks and so on – for a match. According to a recent NBC news investigation, that approach can yield impressive results:

> In Colorado, local investigators have foiled credit-card fraudsters, power-tool bandits and home-garage burglars and identified suspects in a shooting and a road-rage incident…The technology has led to the capture of a serial robber in Indiana, a rapist in Pennsylvania, a car thief in Maine, robbery suspects in South Carolina, a sock thief in New York City and shoplifters in Washington County, Oregon.

It's not just about conventional crime. Driver licenses are the predominant tool of everyday identification, so it's important to prevent their fraudulent issue. Motor vehicle agencies (New York State is one) have used facial-recognition technology for years to combat fraudsters who amass multiple licenses under different names.

Yet doubts about facial recognition linger. Accuracy-wise, it's got a ways to go. Even after all the development, it still works best for white males. Erroneous matches for persons of color and, especially, black women, are depressingly common. But just like Rapid DNA, the sharpest criticism is about the threat that facial recognition poses to civil liberties. "The Perpetual Line-Up," a project of Georgetown Law School, warns that there is "a real risk that police face recognition will be used to stifle free speech":

> Of the 52 agencies that we found to use (or have used) face recognition, we found only one, the Ohio Bureau of Criminal Investigation, whose face recognition use policy expressly prohibits its officers from using face recognition to track individuals engaging in political, religious, or other protected free speech.

Alarm that America will mimic China, where video surveillance is ubiquitous, have led the liberal burg's of Berkeley, Oakland, San Francisco and Sorverville, Massachusetts to ban government use of facial recognition technology altogether. Even Detroit has imposed strict controls. A crime-fraught place where more than four-hundred businesses beam continuous video to police, facial recognition is limited to still photos and violent crimes. So forget about using those video streams! Really, had it not been for Police Chief James Craig's supplications to the city council – he promised that police would compare photos with exquisite care – America's one-time "Motor City" would have likely imposed a total, Berkeley-like ban. Still, his mention that facial recognition had already identified many violent criminals enraged activists, who were upset that the technology had been employed without their assent.

Most recently, facial recognition has taken a hit over its use in – you guessed it – immigration enforcement. According to the *Washington Post*, more than a dozen States

are issuing driver licenses or their equivalents to illegal immigrants. Immigration authorities know that, so they regularly turn to those states' DMV databases to run the photos of, say, absconders who fail to show up for their hearings. That's drawn Georgetown Law's ire. According to Clare Garvier, who led the school's research, "it's an insane breach of trust" for DMV offices to knowingly issue licenses "then turn around and allow ICE access" to the photos.

Technology has given police new tools. It's also taken some away. In "A Dead Man's Tales" we wrote of the FBI's struggle to get Apple to give up the passcode for a dead terrorist's cell phone. (Eventually, the Feebs managed to unlock the device on their own.)

But law enforcement's concerns aren't only about "national security." The Internet is a known go-to place for a multitude of odious pursuits. Say, child sex trafficking. Yet service providers seem strangely indifferent. As Exhibit A, consider Facebook's plan to institute end to end encryption for all its messaging services (WhatsApp, Instagram and Facebook Messenger). Determined to make both sides to conversations impermeable to real-time interception (what we used to call "wiretapping"), humanity's most popular social media platform stubbornly resists the notion of incorporating an electronic "back door."

How to move forward? A recent Carnegie report about the struggle suggests that cops forego intercepting "data-in-motion," that is, as it flows in real time. In exchange, they could get (with a warrant, of course) a pass-key for accessing "data-at-rest", meaning what's present on devices they seize. Of course, from the law enforcement perspective that's hardly sufficient. Stripped of the ability to act proactively, police and the Feds would have to content themselves with collecting evidence after the fact; that is, what the bad guys and girls didn't erase. Preventing crime? Minimizing potentially horrific outcomes? Forgedabboud it!

And that "solution," dear readers, is what preeminent members of the American intelligentsia propose. Good thing they're not crooks!