BIOMETRICS or ... BIOHAZARDS?

John Michael Williams
Bethesda MD USA
+1.301.530.0651
J.Williams@IEEE.org

ABSTRACT

IPSE DIXIT

Biometrics as an array of deployable technologies presumes an elaborate infrastructure, including underlying science that justifies its claims of detection, classification, identification and authentication of individual human identities; particularly of those who are runaways, illegal immigrants, fugitives, criminals, terrorists, and so on.

This will now too often be literally a matter of life and death, both for the public and the individuals identified.

The "New Security Paradigm" emerges from the recognition that the the old paradigm is not securable because it is without scientific substance and/or proof for most of its claims, and composed of inherently inadequate infrastructure, technology, and implementation. Secure biometric applications can't be built from flawed components—one can't make a silk purse from a sow's ear, Irish folk wisdom reminds us. Revolution, not evolution, must be the new paradigm.

To make this case, I begin with a detailed consideration of the "the bedrock forensic identifier of the 20th century," fingerprint identification as practiced in the US, the UK and other advanced societies, for more than 100 years, and which has in many cases been used to establish with "absolute certainty" the identity of some who have paid with their lives. I will demonstrate that the US government has not met its own Supreme Court standards of scientific or technical validity for the FBI or any other fingerprint system, despite partially successful legal maneuvering (but nothing of substance) to reinforce this sine qua non of law enforcement.

I shall then enumerate by trade-name, when available, the significant failures of fingerprint-, iris-, and face-recognition systems, tested this year in Japan and Germany.

The paper concludes with comments on the "bedrock forensic identifier of the 21st century," by an expert witness, the 1993 Nobel Prize winner in Chemistry, and I shall close with a glimpse of the Big Picture, the dismal state of biometrics and related surveillance technology in society at large.

New Security Paradigms Workshop '02, September 23-26, 2002, Virginia Beach, Virginia.

1. PROLOGUE: THE INFOSEC CONTEXT

BIOMETRICS of interest to the Association for Computing Machinery's New Security Paradigms Workshop (ACM's NSPW 2002) automate a portion of the traditional **Identification/Authentication** paradigm:

An individual "user" (accountable active agent, in this case human) is **Identified** (perhaps by assertion), an association that is **Authenticated** by:

- **"Something You Know"**—such as a shared-secret PIN, reusable password or passphrase; single-factor authentication, *extremely weak*, when used alone;
- **"Something You Have"**—such as a key, cryptographic token/one-time password, or smart card; when combined with the above, strong two-factor authentication;
- **"Something You Are"**—Personal recognition by a human security guard, or recognition by automation of some surrogate, such as fingerprint, retina, iris, face, voice, signature or other characteristics. All methods have measurable nonzero **False Positive (F+)** and **False Negative (F-)** rates, whether or not there is enrollment: generally, adjustments to decrease one increase the other. **Lower F+, or lower F- may be preferable,** depending on the application.

when combined with the above, ideal (and most difficult and expensive) three-factor authentication. *Weak to extremely weak if used alone.*

All of the above assume and require:

- A valid, public **science/technology base for the premises such as the diversity of retina or irises or ears,** or peer-reviewed cryptographic algorithms in "trusted" implementations, from which to engineer the automated devices/subsystems, and to which individual products and systems may be compared for efficacy and reliability.
- A **"trusted path"** between all factors used in a particular ID/Authentication and the **"trusted computing base"** performing the validation of the inputs; **realistically, at least minimal tamper/spoof resistance.**

The following will show that **neither criterion is met in almost all "BIOMETRICS"** currently examined by authorities in many countries.

For the first example: even the most time-honored method, that all here probably take on faith, apparently has no "valid, public science/technology base" ...

2. FINGERPRINTS

The "bedrock forensic identifier of the 20th century" [30], is biometric identification of individuals by forensic fingerprinting.

Fingerprint identification in US murder cases has been admissible since at least 1911. The validity of forensic fingerprinting has been challenged in major cases in the US, most recently resulting in Federal opinions in January and March of this year. The historical/explanatory portions of those 2002 decisions are the source of the following analysis [26], [27], unless otherwise noted. The assertions of the court or the Executive Branch represented by the Department of Justice, are in ordinary font; some remarkable assertions, and critical commentary not in the court record are in emphatic font, *thus*.

Presiding Judge Lewis Pollak, a former Dean of Yale Law School [8], rendered **the opinion** and order of January 7 [26], **and reconsideration** of March 13, 2002 [27] in a murder trial in the US District Court for the Eastern District of Pennsylvania, that **ruled forensic fingerprinting in all the forms before the court, especially the FBI's, to be "unscientific"** under Supreme Court standards declared in the Daubert and Kumho Tire cases.

The earlier opinion and order ruled that the "expert witnesses will not be permitted to ... present "evaluation" testimony as to their "opinion" (Rule 702) that a particular latent print is in fact the print of a particular person." The jury would have to determine whether there was a match sufficient to identify the defendant(s)!

In 1993 **the Supreme Court** applied a **standard** in the **Daubert case** for **"scientific evidence"** (later extended in the Kumho Tire case to **"technical evidence"**):

1. **The technique on which the proffered expert testimony is premised "can be (and has been) tested";**
2. **The technique has been "subjected to peer review and publication";**
3. **The technique has "known or potential rate of error. . . and exist[ing] and maint[ained] ... standards controlling the technique's operation"; and**
4. **The technique has "general acceptance" in the scientific community.**

The Daubert and Kumho Tire decisions of the Supreme Court were inspired and informed by the scientific community. The revolutionary decision on admissibility of forensic fingerprinting identification by Judge Pollak, based on Daubert and Kumho Tire, caused a rare (and even more rarely successful) government motion for reconsideration, and provoked strong interest in the scientific community.

The **reconsideration** [27] **orders**, despite the affirmed finding of lack of testing of fingerprinting's premises and methodology, a Daubert essential, and a paucity of support for the remaining three Daubert essentials, **that fingerprinting identification is admissible as specialty testimony, such as accident reconstruction or art appraisal.**

> Note that such specialties *do not usually pretend to identify the defendant at all, much less with "absolute certainty."—see below.*

The order reinstates permission for examiners to testify to the identity of fingerprints.

> *The reconsidered opinion and order (at [27]) is questionable to legal experts and scientists alike (see [8]).*

Forensic fingerprinting has been in development for over 100 years in legal systems worldwide, based on pioneering work in the UK and the US, but was unsound in some instances.

> *In 1924, Scotland Yard revised its fingerprint standards to conform to the findings, published in 1912, of the renowned Alphonse Bertillon of France, which were later conclusively proven to be based on forgeries.*

2.1 FORENSIC FINGERPRINTING ASSERTIONS

2.1.1 FINGERPRINTS FORM EARLY

Fingerprints form in approximately a child's 17th week in the womb. The court took "judicial notice" (i.e., accepted as fact without further argument) the testimony of one scientist, a Dr. William Babler, to this point

2.1.2 FINGERPRINTS ARE PERMANENT

Fingerprints are permanent, throughout the life of individuals, despite trauma to the fingertips.

The court took "judicial notice" (i.e., accepted as fact without further argument) the testimony of that same scientist to this point, since no exception was known, *despite the court's acknowledgment that the scientist considered it "conjecture."*

> *A scientist's "conjecture" fails the Daubert standards as to both testing and known or potential error rate, and thus should be inadmissible, despite its "general acceptance" by an unspecified constituency. Famous science/math conjectures have in fact eventually been disproved [10]*

There is recent evidence that as much as 12 percent of the "user population" may have worn, chemically changed or unscannable fingerprints [11].

2.1.3 FINGERPRINTS CAN BE RELIABLY MATCHED BY HUMANS AND COMPUTERS.

Actual, "rolled" and "latent" prints are reliably matchable, by human and machine methods:

2.1.3.1 IMAGES OF FINGERPRINTS ARE EQUIVALENT TO FINGERPRINTS.

Actual fingerprint patterns are documented by "rolling" each of 10 finger tips, and often the hand and palm, in special ink, then on cardboard, with a practiced collector (such as a police officer) and a cooperative, or at least docile, subject.

The accuracy of rolled representation, or images/reproductions of rolled representations, is not addressed in this record or referenced prior cases as cited. Actual and rolled prints are not distinguished, and thus taken as identical.

2.1.3.2 DEGRADED FINGERPRINT IMAGES CAN BE MATCHED TO HUMAN IDENTITIES.

Crime-scene fingerprint impressions (CSFPI, a designation coined for this paper) are those impressions left by one or more normally-oiled, or sweaty, stained, dirty, bloody etc. fingers by a person on any material from which traces can be captured. These are then "dusted" or otherwise contrast-enhanced as needed, and photographed or "lifted" on transparent tape, etc., for lab processing and analysis: a step which necessarily entails information loss.

These photos or other derivative partial-print images are called "latent" fingerprints (LFP).

The distinction and information loss between CSFPIs and LFPs are not discussed, much less measured. Their identity is tacitly assumed, and only LFPs are discussed.

The possibility of faked or manufactured CSFPIs is not addressed in the record, despite its being feasible with no special knowledge or equipment for more than a century, and a staple of fiction since at least 1895. See for example, Sir Arthur Conan Doyle's "The Adventure of the Norwood Builder":

> When those packets were sealed up, Jonas Oldacre got McFarlane to secure one of the seals by putting his thumb upon the soft wax. ... It was the simplest thing in the world for him to take a wax impression from the seal, to moisten it in as much blood as he could get from a pin-prick, and to put the mark upon the wall during the night...." [2]

"Ian Fleming's Diamonds Are Forever" 1971 film (see http://us.imdb.com/Title?0066995) illustrated a similar ploy, used by Sean Connery's 007 to deceive the femme fatale.

The authorities, including the FBI, are themselves sometimes fabricators of fingerprint evidence [28] and/or corrupters of forensic evidence [25]

2.1.3.3 FINGERPRINTS ARE UNIQUE.

Fingerprints (rolled and latent, the only forms acknowledged) *are unique*: features of the latent print can be compared with hundreds of millions of rolled prints (or their images or digital surrogates) to determine *the unique identity of the latent print with "absolute certainty" (sworn testimony by FBI fingerprint expert, cited at [26])*

"absolute certainty" is an extra-scientific claim, extravagant and without foundation.

Latent prints average only 22 percent or so of the area of the rolled print (inferred from the 50k x 50k study, see below), *and are smudged, smeared, or otherwise marred by the circumstances in which they were deposited, or captured. The error rate in matching must necessarily be high, which is not addressed, or available.*

2.1.3.3.1 The proof in evidence

The proof offered by the US government that fingerprints are "unique" involved only two "experiments":

2.1.3.3.1.1 The Mitchell (FBI) test of state examiner/systems:

Defendant Mitchell's unlabeled rolled prints ("10-print card") and two of his latent prints were sent to all 50 states.

Either the states were surveyed serially, which is highly unlikely, or 1 original and 49, or 50 reproductions of the original rolled prints and latent prints must have been used, with no mention of the mechanism or quality control, if any, of the reproductions.

2.1.3.3.1.1.1 Only Pennsylvania had a hit

Only Pennsylvania, where Mitchell was incarcerated, matched the rolled prints, identified Mitchell—had a "hit."

The prison, public safety and other small populations likely to have fingerprints in state files is a very small fraction of the US, much less world population, and there is no quantification in the record. The state fingerprint files are likely skewed strongly to a preponderance of young, male minorities. That no match occurred in this small number of atypical candidates seems of no statistical significance.

All but West Virginia used automated search and match techniques.

There is no justification given of the automated techniques employed, including such issues as provenance, technology, testing, validation, maintenance and quality assurance—they are all treated as equivalent to human examiners.

2.1.3.3.1.1.2 Remarkable failure rates

Only 30 of 39 states responding claimed to have a match of the rolled prints to both his latent prints; four more matched one latent print to Mitchell's rolled prints; and five matched neither of the Mitchell latent prints to Mitchell's rolled prints.

If the 11 states that failed to respond at all did so because they could not match the latent prints or matched them wrongly, and nine more failed in one or both cases, then 40 percent of the states failed latent-fingerprint matching of the easiest form (i.e.,

only to one "10-print card.") At minimum, 18 percent failed.

It was NOT reported whether any state matched Mitchell's latent prints to any other person, a "false positive," a much more serious error.

2.1.3.3.1.2 The "50k x 50k" Lockheed-Martin (FBI) test

50,000 prints all from white males were compared to each other to "determine the probability that fingerprints of two people could be identical" by Lockheed-Martin, the FBI's builder of the huge, multimillion dollar Integrated Automated Fingerprint Identification System (IAFIS) containing over 400 million fingerprints, recently turned on.

The court record [26] is incomplete: are there 5,000 white males, each with "10-print cards" or 50,000 different males, each with one "full-size, 1-inch" rolled print, or some number in between?—Were different fingers involved, etc.? Did each print have a corresponding artificial partial print (see below)?

The first finding was *"the probability of finding two people with identical fingerprints was one in ten to the ninety-seventh power"—1 in 10^{97}.*

The second finding was that *"the probability of finding two different partial fingerprints to be identical* (artificial partial prints created by using only the center (clean, unsmudged) 21.7 percent of the rolled prints' images] *was one in ten to the twenty-seventh power"—1 in 10^{27}.*

There is no hint of peer review, nor control for organizational-conflict-of-interest (OCOI) in the Lockheed-Martin/AFIS-related findings.

There is no justification given for excluding all but white males, yet drawing inferences for all humanity, for all time.

There is no justification reported for treating perfect artificial partial fingerprints as equivalent to latent fingerprints (LFP), which are normally degraded images of crime-scene fingerprint images (CSFPIs).

There is no justification given of the automated techniques employed, including such issues as provenance, technology, testing, validation, maintenance and quality assurance—they are all treated as equivalent to human examiners.

These extraordinary numbers demand detailed scientific reconsideration. Even the difference, 70 orders of magnitude, strains credulity without extensive review by the scientific community at large.

N.B: The Attorney General of the United States testified before Congress that:

> This funding will be used to improve INS fingerprinting capabilities, and integrate the INS Automated Biometrics Identification System (IDENT) with the FBI's Integrated Automated Fingerprint Identification System (IAFIS). This investment of resources will better equip us to prevent a recurrence of an incident similar to the Rafael Resendiz-Ramirez [an illegal immigrant—not a white male —in Texas] serial killings that occurred in 1999 [1.2].

2.1.4 EXAMINERS AND COMPUTERS IMPLICITLY EQUIVALENT

Determination of fingerprint equivalence may be made by fingerprint examiners, or *computers emulating fingerprint examiners.* FBI new-hires now must have a degree, plus 2 year in-house training, 3-day final exam, and periodic recertification. *All tests are designed, administered and graded by the FBI.*

The FBI's proficiency tests, with "stratospheric success rates," of and by its own examiners, are considered "laughable" by a UK expert (defense witness) who accepts and uses the FBI's ACE-V methodology (see below). This same expert testified to two cases of recent fingerprint misidentification in the UK using ACE-V.

There is no justification given of the automated techniques employed, including such issues as provenance, technology, testing, validation, maintenance and quality assurance—they are all treated as equivalent to human examiners.

2.1.5 THE FEATURES CONSIDERED

Determination of such equivalence is based on feature-analysis techniques, such as matching of loops, whorls, ridges, and "Galton points," usually according to an FBI-adopted "ACE-V" methodology.

2.1.5.1 ACE-V

ACE-V stands for Analysis, Comparison, Evaluation and Verification. The first three activities are performed by a single examiner with varying degrees of automation; the *"Verification"* is usually performed by a second examiner in the same organization who knows the conclusion of the first examiner *(aptly called a "Ratification" by a defense expert witness). The UK requires a third examiner to "verify" as well.*

> There is *no minimum number of feature-matches* standardized or *required by the FBI,* but many feature-matches are required to establish identity in some states and countries, and *the FBI's own Quality Assurance standard "relies on" a 12 feature-match.*

2.1.5.2 SUBJECTIVE IDENTIFICATION

Experts, both using ACE-V, can match most print-features, but still differ on identification. *Identification is acknowledged to be subjective* in ACE-V and all other known methodologies.

2.1.6 NO RESEARCH APPLICABLE

The court writes that research by the National Institutes of Health, the National Institute of Justice or "other institutions both public and private," would be "all to the good," but finds *no current research* (Jain et al. [12] have addressed these issues, largely confirming the lack of credible scientific evidence) and observes that the Executive Branch itself is *just now, 9 years after Daubert, formally soliciting research to establish Daubert criteria for fingerprinting.* [27]

2.2 REACTION TO THE POLLAK DECISIONS

Defense lawyers reacted strongly, as noted in [30]. The American Association for the Advancement of Science (AAAS)

took note of these decisions, and invited a Policy Forum article by a distinguished legal expert, appearing in July in its journal "Science," one of the top two scientific journals in the world, to initiate a debate, which continued in the Letters Section in August [8].

Faigman's comments are excerpted as follows, with particular criticisms in added emphatic font, *thus*.

- *[Pollak's] distinction between science and specialization is premised on a basic skepticism of the scientific method and its usefulness to judicial decision-making*
- *This skepticism stems from ignorance ...*
- To their everlasting shame, [medical,] forensic [and other] scientists also disclaimed the science mantle [to get around "Daubert," to make their testimony admissible]
- ... physicists, biologists, toxicologists, epidemiologists, psychologists, engineers, medical doctors, historians, accountants, auto mechanics, ... This extraordinarily broad array of expertise is simply not susceptible to any one scheme of evaluation... [by judges]
- [Judge Pollak] concluded in the January 7 opinion *that "Daubert's testing factor was not met, and I have found no reason to depart from that conclusion."* (footnote omitted). Yet, somehow, he now [3/2002] found that the other three factors mentioned in Daubert, *error rate, peer review and publication, and general acceptance, were satisfied. How this was possible, without testing, is a great mystery of the decision.*
- [Fingerprinting some judges say] "has withstood the scrutiny and testing of the adversarial process." (footnote omitted). *Scientists undoubtedly will find such an assertion laughable.*
- In doubting the value of the scientific method as the touchstone by which expert evidence is to be evaluated, judges like Pollak and Crow fail to say what should replace it.
- More troubling though, it reflects a basic misunderstanding of the subject of *empirical expertise.* Contrary to Judge Crow's belief, this overreliance on undifferentiated experience does indeed relegate the opinions of testifying experts to *ipse dixit—a Latin phrase that roughly translates as, "because I said so."*
- *To be admissible, fingerprint identification need not be powerful enough to show identity,* but the fact-finder should be given some idea whether one person in 5, or 100, or 1000, could have left the partial print.
- Indeed, failure to put the testing burden on the government creates perverse incentives. If courts admit untested speculation, what incentive does the Justice Department have to do the research? The greater the costs in liberty, lives, and property, the greater should be the expectation that good-quality work be done.
- [For example] general acceptance of polygraphs obviously cannot depend on the views of polygraph operators *any more than the general acceptance of astrology could depend on the views of astrologers.* Moreover, government agencies might generally accept the polygraph because it is a highly useful tool of interrogation. This utility does not mean that courts should accept its validity.
- *... courts can decree that fingerprinting is reliable, but this does not make it true. Only testing will tell us whether it is so.*

Forensic fingerprinting found unscientific above is often concerned with the matching of unknown latent fingerprint(s)—LFP(s)—with a large database—a one-to-many search process. The final ACE-V identification step is subjective.

Another form is the comparison of suspect(s)' rolled 10-print card(s) to crime-scene LFPs—notionally a few-to-few search process. Again, the identification step is subjective.

In employment-background/security checks, 10-print card images may be compared, time and cost permitting, to large databases, but again the identification step is subjective, although the data MAY be of higher quality.

With fingerprint biometric devices, the situation is somewhat different. When an identity is asserted, and fingerprint(s) are offered as authentication of that assertion, the enrolled identity's fingerprint(s) may be retrieved and compared to the offered one(s), a one-to-one search, and a match declared "objectively" with a higher (but unquantified) degree of certainty.

That said, there are still major problems in the theory and practice of fingerprint biometric devices.

3. FINGERPRINT IDENTIFICATION BIOMETRIC DEVICES: *SAYONARA* ...

Tsutomu Matsumoto, a Japanese cryptographer and professor at Yokohama National University, recently presented his findings [18] on 11 commercially-available (but unnamed) systems he and his students tested to demonstrate *the easy defeat of* any reliable or secure fingerprint identification by *any of these gadgets "with a little ingenuity and $10 worth of household supplies."*

His *Gummi-bear attacks* were summarized in [31], which is condensed here:

- Matsumoto uses gelatin, the stuff that Gummi Bears are made of, poured in an easily-made mold of an actual finger, and hardened. The tested fingerprint detectors *make a false-positive identification* of the gelatin fake finger *"about 80 percent of the time,"* falsely identifying the person whose finger was copied.
- He then easily produced a fake finger-with-print from a latent fingerprint by lifting a latent from glass, and enhancing it with a cyanoacrylate adhesive. Next he takes a digital photo, uses PhotoShop for minor tweaks and prints the fingerprint onto a transparency. The transparency is used to etch the fingerprint into the copper of a photo-sensitive printed-circuit board (PCB, available with instructions in most electronics hobby shops), making the print three-dimensional. From this he makes a gelatin finger using the print on the PCB. *This also fools fingerprint detectors about 80 percent of the time. So you could be falsely identified by one of these gadgets, 80 percent of the time, as entering a facility, authorizing a funds transfer, stealing classified documents, etc. by merely leaving a latent print on glass halfway across the world.* [Note the Doyle/Holmes/007 precedents—see above.]
- *Gummy fingers can even fool sensors being watched by guards.* Simply form the clear gelatin finger over your own

(you can moisten the gelatin finger to defeat moisture or electrical resistance sensors), and press your own finger onto the sensor. "After it lets you in, eat the evidence."

- Matsumoto *defeated all 11 commercially-available optical, capacitive, moisture, electrical resistance and "live finger"-detecting fingerprint biometric systems.* He used $10 of ingredients anyone can buy, in the equivalent of a home kitchen. *"The results are enough to scrap the systems completely, and to send the various fingerprint biometric companies packing. Impressive is an understatement."*

4. FINGERPRINT, FACE AND IRIS IDENTIFICATION BIOMETRIC DEVICES: *AUF WIEDERSEHEN...*

The German IT trade magazine named "c't " recently published an in-depth review of a number of biometric devices, and identified them. A translation appeared at extremetech.com, which is the source of this summary. [36]

Eleven systems presented at CeBIT's 2002 trade fair in Hanover were tested: nine fingerprint identifiers, one face recognition and one iris scanning system. Other systems such as "[voice] recognition, hand geometry measurement, signature recognition or keyboard touch dynamics" were excluded because "taken together [they] have only a marginal share of the security biometrics industry's" annual sales.

Primary testing focus: obvious deceptive procedures (such as the reactivation of latent images) and obvious feature forgeries (photographs, videos, silicon fingerprints). They achieved *"astonishing results."* [36]

Secondary testing focus: extraction of biometrically-relevant data by eavesdropping on the communication via the USB port between the computer and the sensor.

The gadgets:

1.) Siemens IDmouse Professional V4.0 with Infineon's capacitive FingerTIP sensor

Defect: Sensor improperly responds to false stimuli, and reactivates latent fingerprint on the sensor's fingertip window.

- *Simple Attack: breathe on a latent fingerprint of an authorized user still on the sensor window to warm it sufficiently* that the sensor considers it live.
- *Simple Attack:* place thin-walled *warm-water-filled plastic bag on a latent fingerprint of an authorized user still on the sensor window*
- *Simple Attack: dust the latent on sensor window with graphite, cover with adhesive film, press gently (nearly 100 percent effective.)*

Defect: Sensor *accepts any* latent print with "high success rate."

- *Simple Attack: lift latent prints from water glass or other surface:* dust latent print with graphite, transfer to transparent film, then *apply to the sensor window with gentle pressure.*

2.) Cherry G83-14000 fingerprint identifying keyboard—same internals as Siemens IDmouse, fell to same attacks.

3.) Eutron (Italy) Magic Secure 3100 capacitive fingerprint identifier and optical USB mouse, from Hunno of South Korea, including a CMOS TouchChip by STMicroelectronics. Somewhat more resistant to "hot breath," but *fell to the same attacks as the Siemens IDmouse.*

4.) Veridicom's 5th Sense Combo, a capacitive fingerprint identifier with a smart-card reader, *fell to the same attacks.*

5. & 6.) Biocentric Solutions (USA) Windows CE and Pocket PC BioHub/BioSentry PDA-based capacitive fingerprint scanners.

Defect: Both samples *extremely defective, tests aborted.*

7.) Identix Bio-Touch USB 200 optical fingerprint identifier.

Defect: Does not detect liveness of finger.

- *Simple Attack: Enroll and authenticate artificial silicone fingertips* made from wax molds (see Gummi-bear attack, above).

Defect: Errs with intense backlighting of fingerprint.

- *Simple Attack: halogen lamp, 30cm from transparent film with lifted latent print,* increases image contrast and "snow-blinds" the scanner successfully, *so the device accepts latent as live.*

8.) Cherry G81-12000 keyboard with optical fingerprint identifier made by Identix (see above) *has "more or less identical" defects and attacks.*

9.) IdentAlink's Sweeping (thermal) Fingerprint Scanner FPS100U using Atmel's CMOS-Finger-Chip-Sensor FCD4B14, and BioLogon software.

Defect: Defective BioLogon software, and live finger sensing defeated with effort.

- Simple Attack: Copy enrolled fingerprints in silicone, then use fake fingers to match.
- Subtle Attack: Enroll silicone prints of intruders, then identification later of real intruders is automatic.

FASCHING MASKS?

10.) Panasonic's Authenticam BM-ET100, an iris scanner that has been marketed for some time in the USA, involving two dim and one bright infrared beam directed at the enrollees' and subjects' iris (alienating to voluntary enrollees), bundled with Iridian's PrivateID software.

Defect: uses pupil aperture and depth to determine liveness, then performs iris-analysis/matching/recognition.

- *Simple Attack:* take high resolution picture of enrolled eye(s), make inkjet 2400x1200dpi image, cut pupil hole, intruder looks through hole in *"artificial eye" mask,* providing pupil aperture/depth, but enrollee's iris pattern—*anyone can be recognized as enrollee.*
- *Subtle Attack: Enroll with "artificial eye(s)",* then both masked intruder and original may be recognized.

11.) The FaceVACS-Logon device, by Dresdner Cognitec AG, performs "face recognition" by storing 2D representations of facial images, nonunique digital surrogates, during enrollment, and searches the Enrollment database for matches when new faces are presented, both via ordinary webcam. As the name implies, it is intended to authenticate computer logon.

Defect: Photo matches the database.

- *Simple Attack: Use photo print, or image on notebook screen, to match.*

Defect: Enrollment files are stored without protection, with global access.

- *Simple Attack:* Copy enrollment files to notebook, *display any real, photo, or derived image on notebook screen* that encodes to the same surrogate(s).
- *Subtle Attack: Insert image surrogates of intruders* into the Enrollment database, to ease future intruder recognition.
- *Subtle Attack: Delete or corrupt database image surrogates, to either impair recognition of particular individuals, or create errors so numerous that the system is turned off completely, and/or discredits security personnel/operations.*

Countermeasure: Activate Liveness Test: requires slight movement in "face" to match.

Defect: Slows valid face matches considerably, has more false-negatives, facial movement insufficient discriminator.

- *Simple Attack: Short video (.avi) image on notebook's screen is accepted as live.*

Defect: Low-resolution images result in false-positives.

- *Simple Attack: Shoot three low-resolution images of an already-enrolled face* in high, medium, and low light, *then display same composite face on notebook screen*

"All the weaknesses [identified above] *are in part those of the algorithms used and not those of the sensors applied."* [36]

12.) USB sniffing:

Defect: Most of these devices above interface via the Universal Serial Bus, USB. It can be monitored to extract all essential biometric information for later attacks.

- *Simple Attack:* Install "USB Snoop for Windows" filter driver, and/or "USB Agent" by Hitex software packages in/near Windows host, and capture all device transmissions (actually done on Siemens IDmouse) in a log, analyze, *extract real images*, etc.

Caveat emptor.

Note: Microsoft has announced biometric plans (for instance, see "Microsoft and I/O Software ... Cooperate to Develop Biometrics Technology for Integration In Future Versions of Windows" at http://www.microsoft.com/presspass/press/2000/May00/BiometicsPR.asp), but tests of its products were not available.

5. DNA TESTING

If fingerprinting is "the bedrock forensic identifier of the 20th century," surely the "bedrock forensic identifier of the 21st century" is DNA testing.

But consider *the O. J. Simpson double murder trial*, in which identification of his DNA was central to the prosecution's case against him, and in the opinion of the inventor of the PCR/DNA technique, *is typical of forensic DNA identification he has examined.*

The defense hired Dr. Kary Mullis, 1993 winner of the Nobel Prize in Chemistry for the invention of the polymerase chain reaction, the PCR process, that has made testing of minute, trace quantities of DNA, amplified by PCR, comparable to known DNA samples drawn from suspects, victims, etc. Mullis writes:

> I testified in [previous] murder trials for the defense, and I felt that my role there was to make sure the PCR-DNA work had been done fairly and correctly. I was not there to be on someone's side. *I found in almost every case that the testing protocols did not stand up under careful scrutiny and that the errors were neither inconsequential nor insubstantial ...*
>
> ... just finding DNA at the scene of a crime that resembles a suspect's DNA in every way you have examined it could mean many things. If you find the first two numbers of a Social Security Number you can prove it's not mine if it doesn't match, but you can't prove it is mine if it does. You need the whole thing to do that. *DNA evidence as obtained by forensic labs* is only the first two numbers. It *has its limitations*. [19]

In the OJ case, Mullis concluded:

- The LAPD DNA lab "had some of the right tools but by no means all the right tools."
- The staff were untrained, inexperienced, and immature ("fresh out of college").
- The LAPD DNA evidence should have been *"thrown out on first principles ... of science that had been clearly established by the end of the seventeenth century."*

Specifically:

- There was no safeguard against innocent or malign researcher/evidence-gatherer/tester bias, such as:
- no "blind" study provisions, such as storing OJ's blood in a coded vial, without his name in plain view and known to all conducting tests;
- no "control group" blood samples from known innocents at the same time and place that OJ's were taken, also encoded so that identities are hidden, and errors if any would be common to all;
- no collection-process safeguards (such as defense counsel present when samples collected), to preclude later disputes on the sampling itself.
- There was no tagant (like a simple food dye, or better, a DNA tracer made for the purpose). Tagants "can't be removed without removing the DNA itself," to preclude chain-of-custody arguments, like the one used against Inspector Lang, because he "had kept an envelope [with a test tube of OJ's blood] on the back seat of his car for several hours." Johnny Cochran persuaded the jury it could have been used to plant OJ's blood at the scene, undermining the prosecution's DNA evidence and obviating Mullis's taking the stand.

So many failures in rigor in so many well-financed trials (and even in routine paternity suits [19]) do not bode well for the "the bedrock forensic identifier of the 21st century," at least as a tool of the prosecution.

6. THE BIG PICTURE: *SAY CHEESE*

In the opinion of major system integrators (for example [37]), fingerprint ID gadgets are the most widely used, and cheapest, but have high error rates.

- New York state uses fingerprint ID for welfare applicants [11].

- The USDA has mandated the technique for food-stamp clients in some pilot programs, reducing fraud, but driving away clients [7].
- Hairdressers and others who work with strong chemicals, and the elderly often can't be scanned due to worn prints, and the size of this population has been measured to be "12 percent of users" [11].
- There are massive efforts for DoD, national and international ID cards, perhaps supplanting drivers' licenses, passports, Social Security and other documents [16].
- DoD has already deployed smart-cards for related ID/Authentication, of a class whose vulnerability has recently been disclosed (the flashbulb attack) [16].

Iris identification (the received notion is that it is better than fingerprint, but invasive, and most expensive [37]) if put to the Daubert/Supreme Court test, would probably be found unscientific, at least with respect to its claim that all irises are unique at the level of resolution of available and practical scanners. A principal academic exponent is John Daugman of the University of Groningen, currently at the University of Cambridge Computer Laboratory [5], who is among those building both an experimental and theoretical basis for a scientific assessment for this specialty. It is increasingly used in high-security environments, such as inmate ID in advanced prisons [17.2].

Hand-geometry matching devices are gaining in deployment, if not acceptance:

- DisneyWorld's custom-built, low F- hand geometry gate control is well suited for high-volume traffic of mostly-honest ticket holders, and a security expert's personal informal observations and tests over an extended period, and discussions of the system [10] strongly support and amplify the results reported by the Company [13], in turn showing that very carefully designed and implemented biometric systems can provide significant economic advantage.
- However, the low F- and higher F+ make the Immigration and Naturalization Service's choice of hand-geometry for another potentially high-volume application, INSPASS for frequent air travelers [11], questionable, unless it was subjected to rigorous testing and analysis comparable to DisneyWorld's.
- **New York-Presbyterian Hospital employees smashed slow hand-scanners, in frustration, two weeks in a row recently [11].**

Automated facial-recognition is scheduled for worldwide, large-scale deployment for anti-crime, counterterror despite:

- Tampa's Visionics/Identix face-scanning of Super Bowl fans bombed, and scanning of its entertainment district gave no hits, high F+ [7], [11], [38].
- The Statue of Liberty visitors are face-scanned [7].
- **No US arrests are attributed to face-scanning, as of 9/13/02 [9].**
- A test of Visionics/Identix at Palm Beach (FL) International Airport let over half the faces in its mock-terrorist database (presumably rigged with perfect photos) go unchallenged, but 1 in every 100 was falsely labeled "terrorist," when there may actually be 1 terrorist in 107 passengers: **a 5-order-of-magnitude error rate, minimum** [4].
- Identix claims its face-recognition product has F+ of 0.68 percent (again, assuming perfect-picture enrollment). At Boston's Logan, with 25,000,000 passengers per year, it would have a **minimum false terrorist-accusation rate of 500 per day** (far greater, if matching against poor-quality, grainy, low-light, oblique terrorists' images) [15]. RAND's proposals for a "Potemkin Village" of face-scanners with or without multistage processing are implausible improvements [38].
- Providence RI's international airport, first to plan face-scanning, rejected it as unsound and prone to F+ [7].
- Australia's FaceLab is a prototype face-scanner being tested by every major global car company, to **monitor for sleepy, inattentive drivers** [14].
- Face Recognition Verification Tests (FRVT 2000) by NIST, DARPA et al. bombed. FRVT 2002 results are due soon. [23]

Camera surveillance is spreading rapidly, and is the vanguard of face-recognition:

- DC, Norfolk and Virginia Beach VA, the state of Kentucky, Australia, and New Zealand, are implementing CCTV crime programs that can be converted to face recognition [Glanz, [29].
- DC's and other traffic-camera programs are operated for public and private revenue, more than traffic safety [6]
- **"An average American is caught on camera eight to 10 times a day..." [35]**
- The UK has installed at least 40,000 CCTV cameras and/or increased street lighting in England and Wales, (up to 1.5 million total have been reported for the whole UK, notably including Northern Ireland, Scotland and various possessions), for counterterrorism;
- estimate: **the average Londoner's picture is recorded more than 300 times a day**;
- the Labor government claims the program and its deterrence produced a 20 percent reduction in street crime, but a major independent study reported only 5 percent reduction over the same period, mainly in car theft, not violent crimes, and mainly through deterrence, not arrests [7], [1.1]
- Microwave *peeping-Toms* may now be at some airport gates, *cameras* that see through clothing, displaying all including detailed genitalia (no open discussion on whether this provides a new opportunity for recognition algorithms, such as for faces and irises), have been proposed for airport security [21] despite warnings from the National Research Council that "possible negative public reaction toward many of these new detection technologies will have to be addressed before these systems can be used in airports" [24]. Privacy/modesty-protecting versions have also been proposed [33]. One hopes that their operation remains covert, in both senses.
- The cameras have bred simple countermeasures [22].

Some identification technology with immense tracking and privacy implications, may be used to supplement biometrics:

- Saudi Arabia is using Russian technology with *RFid tags (radio-frequency transponders)* buried in the visa of pilgrims to Mecca, to monitor their movements in country [32].

When these technologies are recommended for government-wide, or nationwide use as in "National ID cards" being strenuously promoted on the first anniversary of 9/11, cooler heads have issued grave warnings, in particular the National Academy of Sciences/National Research Council, in its report this spring. My fellow panelist Bob Blakley will discuss this report to which he was an important contributor, so here it suffices to mention that the section entitled "Binding Persons To Identities" [3] enumerates many of the problems encountered with "biometrics" of the type discussed here when combined with the challenge of binding on this scale—or even in smaller, for example, state-wide/driver's license and similar systems.

Such sage advice will not appeal to the "lunatic fringe," nor likely dissuade governments from deploying *exotica*:

- NASA proposed to use "noninvasive *neuro-electric sensors*," imbedded in airport gates, to collect tiny electric signals that all brains and hearts transmit—that is, *to read minds*. Computers would apply statistical algorithms to correlate physiologic patterns with computerized data on travel routines, criminal background and credit information from "hundreds to thousands of data sources," NASA documents say [20].

Were this latter notion remotely feasible, it should have long ago been applied to the *perennially discredited "biometrics" of polygraphic "lie detection,"* so severely criticized and rejected in a current National Academy of Sciences/National Research Council report "The Polygraph and Lie Detection" [24]. While its investigative utility "when used with respect to specific incidents—as in criminal probes, where a suspect is asked whether he committed the crime" is acknowledged, it is no better than a "placebo" in other circumstances—*it has NEVER caught a spy, the report emphasizes*. Fortunately, it is usually inadmissible by the prosecution, although in Maryland, for instance, the defense may introduce polygraph results, whereupon it is fair game [17.1]. The print press took note editorially [39], but it is unlikely its spreading use by governments of all stripes will decline post-9/11.

Other forms of biometric "lie detection" such as thermal imaging of the eyes proposed by the Mayo Clinic [34] *are as yet unscientific by the Daubert/Supreme Court standard*, and some, like voice stress analyzers, have been retired by responsible authorities [17.1].

True stories?

Cops were having trouble getting a suspect to confess, so one deputy brought in his colander and some alligator clips with a heavy extension cord attached. After placing the colander on the suspect's head, with the alligator clips attached, they took the extension cord around a corner and "plugged it in." After telling him "the machine" proved he had lied, the suspect confessed.

Cops in a different jurisdiction walked the suspect up to the office copier, placed his hands on the glass, then both sides of his face, took the copies, and disappeared for 20 minutes. When they returned, saying the printouts proved he was lying, he confessed.

Just as effective, and deceptive it seems, as these "Potemkin" gadgets, and a lot cheaper.

There is little technology, less science, and no security behind too many of the products; the vendors' offers are *ipse dixit*—sows' ears.

7. ACKNOWLEDGEMENTS

My initial suggestion for a Panel for NSPW 2002, "Biometrics considered harmful!," produced many provocative replies. Interesting exchanges with General Chair Cristina Serban, fellow panelists Carla Marceau and Bob Blakley, and major contributions by recuperating Marv Schaefer and by Panel Chair Steve Greenwald, with many cogent comments from the workshop itself documented by Steve and Mary Ellen Zurko, were integrated in this reference for our security research community. That it appears in this Proceedings at all is partly through the good work (and indulgence) of Victor Raskin, Publications Chair.

All errors and omissions are mine. As a panel/discussion paper it is neither formally scientific, nor a polemic, nor is it "balanced" in the journalistic sense: it is a debater's argument in the affirmative that "Resolved: Biometrics considered harmful!" is presently the prudent proposition. As much as others contributed, this position is mine, not that of NSPW.

It is offered with hope for "silk purse" high-quality technology, based on high-quality computer and biological science, to emerge in the biometrics field.

It is a matter of life and death.

8. REFERENCES

[1.1] [Armitage] "To CCTV or not to CCTV," Rachel Armitage, National Association for the Care and Rehabilitation of Offenders (NACRO, a UK charity) Crime and Social Policy Unit, London, May 2002, http://www.nacro.org.uk/templates/news/newsitem.cfm/2002062800.htm

[1.2] [Ashcroft], "ATTORNEY GENERAL JOHN ASHCROFT'S TESTIMONY BEFORE THE SENATE COMMITTEE ON APPROPRIATIONS: The President's FY 2002 Budget Request for the Department of Justice," April 26, 2001, http://www.ins.usdoj.gov/graphics/aboutins/budget/0402601ag.htm

[2] [Baring-Gould] "The Annotated Sherlock Holmes/The Four Novels and the Fifty-Six Short Stories Complete, by Sir Arthur Conan Doyle," William S. Baring-Gould, 1967, Clarkson N. Potter Inc. Publisher - New York, Second Edition, 1977. Baring-Gould notes (Vol. II, pg. 425) that Holmes/Doyle was aware of fingerprints and their importance in detection (and apparently, their easy substitution), as of 1895, well before their adoption by Scotland Yard.

[3] [Blakley] "IDs - Not That Easy: Questions About Nationwide Identity Systems," Bob Blakley et al., NATIONAL RESEARCH COUNCIL, Division on Engineering and Physical Sciences Computer Science and Telecommunications Board, COMMITTEE ON AUTHENTICATION TECHNOLOGIES AND THEIR PRIVACY IMPLICATIONS, 4/11/2002, see http://www4.nationalacademies.org/news.nsf/0a254cd9b53e0bc585256777004e74d3/b875c695fdc5e77585256b98006e9cf7?OpenDocument , and available at http://www.nap.edu/books/030908430X/html/; for "Binding Persons To Identities," see

http://books.nap.edu/books/030908430X/html/37.html#page top

[4] [Cherry] "BIOMETRICS - Who Goes There?," Steven Cherry, IEEE Spectrum, September 2002, http://www.spectrum.ieee.org/WEBONLY/resource/sep02/911e.html

[5] [Daugman] "How Iris Recognition Works," John Daugman, http://www.cl.cam.ac.uk/users/jgd1000/irisrecog.pdf

[6] [DeBose] "AAA pulls its support for DC traffic cameras; Spokesman furious after mayor cites revenue priority," Brian DeBose, The Washington Times, October 17 2002, http://www.washtimes.com/

[7] [EPIC] "Face Recognition," anonymous, Electronic Privacy Information Center, http://www.epic.org/privacy/facerecognition/ as of 9/21/02.

[8] [Faigman] "SCIENCE AND THE LAW: Is Science Different for Lawyers?," David L. Faigman, Science, Volume 297, Number 5580, Issue of 19 Jul 2002, pp. 339-340 at http://www.sciencemag.org/cgi/content/full/297/5580/339 D. L. Faigman is a professor of law at the Hastings College of the Law, University of California, San Francisco, CA 94102, USA. E-mail: faigmand@uchastings.edu

The Letters Section of 23 August at http://www.sciencemag.org/cgi/content/full/297/5585/1275b contains a comment on this Policy Forum entitled "Many Courts Still Frye Scientific Evidence," from Leonard Deftos, Department of Medicine, University of California at San Diego/SDVAMC, who reports the continued use of the Frye standard in some state courts, notably California, but largely endorses Prof. Faigman's position.

[9] [Glanz] "Mugging for the cops," William Glanz, THE WASHINGTON TIMES. 9/13/2002, http://www.washtimes.com/business/20020913-96526518.htm

[10] [Greenwald] Private communication re conjectures, Dr. Steven J. Greenwald, 9/8/2002. Dr. Greenwald affirmed many science/math conjectures have been refuted, citing from memory Lord Kelvin's Conjecture about 12 years ago, and Euler's Sum of Powers Conjecture about 35 years ago.

Private communication re DisneyWorld's hand geometry admission-control system, 10/18/2002.

[11] [Hawkins] "Body of Evidence," Dana Hawkins, US News & World Report, February 18, 2002, pp 60-62.

[12] [Jain] "On the Individuality of Fingerprints," S. Pankanti, S. Prabhakar, and A. K. Jain, "IEEE Transactions on PAMI, Vol. 24, No. 8, pp. 1010-1025, 2002. A shorter version also appears in Fingerprint Whorld, pp. 150-159, July 2002. See also http://biometrics.cse.msu.edu/

[13] [Levin] "Real World, Most Demanding Biometric System Usage," Gordon Levin, The Walt Disney World Company, in the Proceedings of the Biometrics Association Conference, 2/13-15/2002, Crystal City VA, NISTIR 6755, http://www.itl.nist.gov/div895/isis/bc/bc2001/home.htm

[14] [Mahne] "Big Brother watches you drive," Christian Mahne, BBC News Sydney Australia, 9/9/2002, http://news.bbc.co.uk/1/low/technology/2246115.stm

[15] [Mann] "Homeland Insecurity" (10+ page interview and profile of security expert Bruce Schneier), Charles Mann, The Atlantic Monthly, September 2002, http://www.theatlantic.com/issues/2002/09/mann.html

"Why Software Is So Bad," MIT Technology Review, Charles C. Mann, July/August 2002 http://www.technologyreview.com/articles/mann0702.asp?p=0

[16] [Markoff] "Vulnerability Is Discovered in Security for Smart Cards," John Markoff, The New York Times, May 13, 2002, http://www.nytimes.com/2002/05/13/technology/13SMAR.html

See also "High-tech ID eyed for global seafarers," John Zarocostas, WASHINGTON TIMES, October 30, 2002, http://www.washtimes.com/business/20021030-4759208.htm

See also "NSA will test a high-level access card," Dipka Bhambhani, 10/09/02, Government Computer News, http://www.gcn.com/vol1_no1/daily-updates/20233-1.html

[17.1] [Marquez] Private communication, Detective Miguel A. Marquez, Coordinator/Examiner, Polygraph Unit, Forensic Services Section, Montgomery County Maryland Police Department; 10/17/2002.

[17.2] [Marlatt] Private communication, Sgt. D. Marlatt, Montgomery County Maryland Department of Corrections and Rehabilitation, 11/6/2002, regarding the $90 million, state-of-the-art county jail to be occupied soon. See also "Security Bugs Push Back Jail Opening To Early '03—System Readjustments Needed, Officials Say," Phoung Ly, The Washington Post, 11/07/2002, http://www.washingtonpost.com/wp-dyn/articles/A17043-2002Nov6.html

[18] [Matsumoto] "Impact of Artificial Gummy Fingers on Fingerprint Systems," T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, Proceedings of SPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, 2002.

[19] [Mullis "Dancing Naked In the Mind Field," Kary Mullis, Pantheon Books, New York, 1998. See especially "Fear and Lawyers in Los Angeles," pp. 45-62.

See also "Paternity Tests Yield Conflicting Results ñ Contradiction Sparks Concern About [DNA] Methods Used in Thousands of DC Support Cases," Sewell Chan, Washington Post, 10/28/2002, page B1

[20] [Murray, F.] "NASA plans to read terrorist's minds at airports," Frank J. Murray, THE WASHINGTON TIMES, 8/17/2002, http://asp.washtimes.com/printarticle.asp?action=print&ArticleID=20020817-704732

[21] [Murray, C.] "Wanted: Next-gen tech for weapons detection," Charles J. Murray, EE Times, September 17, 2001 at http://www.mwee.com/mwee_news/OEG20010917S0048

[22] [Naimark] "How to Zap a Camera," Michael Naimark, counter-surveillance research of the Institute of Advanced Media Arts and Sciences (IAMAS), Gifu, JAPAN (2002), at http://www.naimark.net/projects.html

[23] [NIST] "Face Recognition Vendor Tests. FRVT", 2000, 2002, National Institutes of Standards and Technology, http://www.frvt.org/FRVT2002/Default.htm

[24] [NRC] "The Polygraph and Lie Detection," NATIONAL RESEARCH COUNCIL, Division of Behavioral and Social Sciences and Education, Board on Behavioral, Cognitive, and Sensory Sciences and Committee on National Statistics, Committee to Review the Scientific Evidence on the Polygraph; 10/8/2002, see

http://www4.nationalacademies.org/news.nsf/0a254cd9b53e0bc585256777004e74d3/0b706678c4901fcc85256c4c005065d0?OpenDocument ; the report itself is at http://www.nap.edu/books/0309084369/html/

"Airline Passenger Security Screening: New Technologies and Implementation Issues (1996)," Commission on Engineering and Technical Systems (CETS), at http://www.nap.edu/books/0309054397/html/13.html

[25] [NYSDA] "FBI Lab Revelations Endanger Cases," anonymous, New York State Defenders Association, February 1997, http://www.nysda.org/Publications/The_Report/0297.html

FBI labs falsification of forensic reports led to "fifty prosecutors [being] notified of cases in which problems might be raised by the defense, according to The New York Times." http://www.nysda.org/Publications/The_Report/0297.html,

[26] [Pollak 1/2002] IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA :v. : Cr. No. 98-362-10, 11, 12

CARLOS IVAN LLERA PLAZA, WILFREDO MARTINEZ ACOSTA, and VICTOR RODRIGUEZ, January 7, 2002.

The opinion and order are at: http://www.paed.uscourts.gov/documents/opinions/02D0046P.HTM

[27] [Pollak 3/2002] IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA :v. : Cr. No. 98-362-10, 11, 12

CARLOS IVAN LLERA PLAZA, WILFREDO MARTINEZ ACOSTA, and VICTOR RODRIGUEZ, March 13, 2002.

The reconsideration is at http://www.paed.uscourts.gov/documents/opinions/02D0182P.HTM

[28] [Roth-Kinge] "Final Report on Trooper Evidence Tampering ," Nelson Roth, February 1997, mentioned at The New York State Defenders Association, http://www.nysda.org/Publications/The_Report/0297.html, which recounts the police falsification of fingerprint evidence in the Shirley Kinge case, incarcerated in 1991 for complicity in a quadruple-murder cover-up, and exonerated many years later. Another account may be found in the New York Times for February 4, 1997, "Supervision of Troopers Faulted In Evidence-Tampering Scandal" discussing, among others, "... six troopers [who] fabricated evidence, usually by planting fingerprints ..."—at http://query.nytimes.com/search/abstract?res=F30C10FD35590C778CDDAB0894DF494D81

In 2001 Kinge was still suing the state of New York for wrongful prosecution, as noted in http://www.theithacajournal.com/news/stories/20010101/opinion/149933.html

[29] [Roy] "New cameras to catch trash scofflaws in act," MATTHEW ROY, The Virginian-Pilot, September 19, 2002, http://www.pilotonline.com/news/nw0919dum.html

[30] [Scheck] "Will Fingerprinting Stand Up in Court?," Barry Scheck and Peter Neufeld; The New York Times, March 9, 2002, pg. A15 OpEd. Neufeld and Scheck, who direct Cardozo Law School's Innocence Project (and who coincidentally recruited Dr. Mullis [19]), took the January 7 opinion [26] as the point of departure.

[31] [Schneier] "Fun with Fingerprint Readers," Bruce Schneier, Crypto-Gram, http://www.counterpane.com/crypto-gram-0205.html

[32] [Schwartz] "Eerie possibilities," Ephraim Schwartz, InfoWorld, 9/6/02

http://ww1.infoworld.com/cgi-bin/fixup.pl?story=http://www.infoworld.com/articles/op/xml/02/09/09/020909opwireless.xml&dctag=wireless

[33] [SD] "The People Portal microwave security scanner," Spatial Dynamics, Inc., February 08, 2002, http://www.spatialdynamicsinc.com/prod03.htm

[34] [Slotnick] "Diogenesí New Lamp," Rebecca Sloan Slotnick, American Scientist - Science Observer, March-April, 2002, see http://www.sigmaxi.org/amsci/Issues/Sciobs02/sciobs0203deception.html

[[35] [Sorokin] "Sniper likely passed camera," Ellen Sorokin, THE WASHINGTON TIMES, 10/18/2002 http://www.washtimes.com/metro/20021018-13730040.htm

There has been at least one report that a red-light camera "caught on film" the sniper's tag numbers, but with no indication that this was material in the capture of the murder weapon and the arrest of two in the shooting of 14 rounds, killing 10 and wounding three in the Washington DC environs during a 3-week period in October 2002; see Frank J. Murray, "A tight noose ," THE WASHINGTON TIMES, October 27, 2002, page 1. http://www.washtimes.com/national/20021027-868849.htm

[36] [Thalheim] "Body Check: Biometrics Defeated," Lisa Thalheim, Jan Krissler, Peter-Michael Ziegler, June 3, 2002; Reprinted with permission from c't Magazine, translated from the German by Robert W. Smith. http://www.extremetech.com/article/0,3396,s=1024&a=27687,00.asp ; see also http://www.heise.de/ct/english/02/11/114/

[37] [Unisys] "The Potential of Biometrics," Ed Schaffner, Exec Magazine (Unisys publication), V24N3 2002, pg. 13. See http://www.unisys.com/

See also "Biometric Technologies ... Emerging Into the Mainstream" R. M. Bolle et al., October 12, 2001, IBM Research Report RC22203 (W0110-041), IBM Research Division, Thomas J. Watson Research Center, P.O. Box 218, Yorktown Heights, NY 10598

[38] [Woodward] "Biometrics ñ Facing Up To Terrorism," John D. Woodward, Jr., RAND Corporation Monograph, 22pages, http://www.RAND.org, 2001.

"SuperBowl Surveillance ñ Facing Up To Biometrics", John D. Woodward, Jr., The Intelligencer ñ Journal of U. S. Intelligence Studies, V12N1, Summer 2001, Association of Former Intelligence Officers, pp 37-43, reprint permission via http://www.RAND.org/organization/ard/

[39] [WPWT] "Are Polygraphs Lying?," Washington Post Editorial, Thursday, October 17, 2002, Page A20; "The truth is polygraphs lie," Washington Times - Steve Chapman, October 16, 2002, at http://www.washtimes.com/commentary/chapman.htm; and "Spies, lies and polygraphs," Washington Times - Drew Richardson, October 17, 2002, at http://www.washtimes.com/op-ed/20021017-15032558.htm