The Expanding Surveillance State:

Why Colorado Should Scrap The Plan To Map Every Driver's Face and Should Ban Facial Recognition In Public Places

By Mike Krause

Issue Paper
Number 8-2001
October, 2001

Executive Summary

"To be governed…is to be watched, inspected, directed, indoctrinated, numbered, estimated, regulated, commanded, controlled, law-driven, preached at, spied upon, censured, checked, valued, enrolled by creatures who have neither the right, nor the wisdom, nor the virtue to do so."

Pierre-Joseph Proudhon

As a whole, we citizens routinely hand over large amounts of personal and intrusive information to the state as a matter of law. Whether to obtain a license, to comply with the police officer who has just pulled you over, or to tell the tax man how much money we make, it seems that we are always handing over another bit of information about ourselves.
The Colorado legislature last year introduced us to the next generation of surveillance technology, facial recognition, in a nation already under intense scrutiny.

Indeed, the amount of government-compelled information on citizens, gathered not as part of any criminal investigation but rather as a matter of routine, has become immense. In a recent Washington, D.C.-based Cato Institute (www.cato.org) briefing paper, "Watching You: Systematic Federal Surveillance of Ordinary Americans" (http://www.cato.org/pubs/briefs/bp-069es.html), Boise State University Professor Charlotte Twight provides a partial list. This list includes employment histories, income, childhood and subsequent educational experiences, medical histories (including doctors' subjective impressions), financial transactions (including copies of personal checks written), ancestry, rent and mortgage payments just to name a few.

Here in Colorado, the Department of Revenue bundles up and sells government-compelled information. This includes names, addresses, dates of birth, driving records, restrictions and other information associated with your license and vehicle registration. (www.i2i.org/Publications/Op-Eds/PersonalFreedom/driverdata.htm)

Nearly all of this government-compelled information is now keyed in to the Social Security number, as a "unique identifier."

Every new database, every new surveillance tool is usually accompanied by the promise of some new benefit. It will make us safer, fight fraud and other crimes, stop illegal immigration and make government more efficient. And of course, privacy concerns are always assuaged with the promise of strict oversight.

Yet invariably, these measures are used for purposes other than those promised. Rather than making government more efficient, they instead fuel the growth of ever bigger and more intrusive government.

In 'Watching You', Professor Twight shows how this works. With the expanding Surveillance State has come routine "data swapping" by various government agencies. Some of the agencies routinely exchanging information about us are:

- The IRS and the Social Security Administration (SSA)
- SSA and the Health Care Financing Administration
- The Postal Service and the Department of Labor
- The Justice Department and the Department of Veterans Affairs
- The IRS and state social services agencies
- The Department of Education and the Department of Health and Human Services
- The Social Security Administration and State Courts

It is not clear that the net effect of all this is more efficient government or less fraud, crime and illegal immigration, but rather more general scrutiny of the population by their government. Law Professor Paul Swartz is quoted in ‘Watching You’, “Americans no longer know how their personal information will be applied, who will gain access to it and what decisions will be made with it…Individuals whose personal data are shared, processed and stored by a mysterious bureaucracy will be more likely to act as the government wishes them to act.”

This matters because, in America, the government is supposed to be the servant and not the master.

The promises of facial recognition have been the usual: fight fraud, reduce crime, stop illegal immigration, etc. But interestingly enough, its proponents have spent as much, if not more time explaining how it will not be used as they have expounding on its virtues. This is evidence that more and more people, including many in government, are questioning the need for a new expansion of the Surveillance State.

This paper will examine the potential use and abuse of facial recognition in conjunction with existing government databases, its efficacy, its place (or lack thereof) in a free and open society, and the proposed use of facial recognition in Colorado.

Introduction

This spring, the Colorado legislature approved, and the governor signed, legislation to allow the Division of Motor Vehicles to use biometric technology to facially map or "face print" Colorado license applicants.

In July, lawmakers found themselves on the defensive when it was revealed that the legislation allowed for unrestricted use of the DMV database by any government agency that cares to take a peek. The governor has expressed consideration of an executive order to tighten things up and several lawmakers have promised legislation (new laws on top of new laws) to make sure facial mapping is used only for its intended purpose. (1)

Is This Supposed to Make Everything OK?

Whatever good intentions are behind the face-print database, they have been overshadowed by the actions of government in another state.

This year, at Super Bowl XXXV, police in Tampa, Florida used face scanning and facial recognition technologies to surreptitiously scan and capture images of football fans to compare against an existing database of digital photos.

There is nothing new about the use of surveillance tools in contemporary America. Indeed we are routinely under surveillance while going about our daily lives. At the bank, in parking lots, while shopping and even while pumping gas, we are under the scrutiny of the camera. Moreover, facial recognition technology is nothing new. It has been in use in a limited capacity for some time now, by the Department of Defense, agencies of the federal government, some private sector industries and by governments in other countries.

There is also nothing inherently wrong with the use of technology by government. Police in Colorado have used video cameras to help identify and track down rioters on several occasions and images captured by citizens in the right time at the right place have proved to be valuable to law enforcement.

Also, some government applications of facial recognition and face scanning systems have merit. Regulating access to criminal evidence, weapons arsenals or nuclear materials, for example, may be ideally suited for biometrics. And the limited use of facial recognition against a database of known or suspected terrorists in airports may prove to be a highly effective and efficient security measure.

Moreover, closed circuit TV cameras are often used to monitor traffic and crowds. But CCTV can't be used to instantly match a face to a database and create an electronic dossier. But the combination of facial scanning and recognition software deployed in public spaces and a biometrically "mapped" database of every licensed driver in the state combined with the accompanying DMV information (or combined with other state agency databases such as police agencies or revenue departments) represents a new level of surveillance and potential abuse that, above and beyond the privacy issues raised, could usher in new levels of intrusion into the lives of Coloradans and an unnecessary expansion of government power.

I am not alone here. This July, conservative House Majority Leader Dick Armey (R-TX) joined with the American Civil Liberties Union to raise the alarm about the rise of the surveillance state. Colorado's plan was specifically mentioned: "Used in conjunction with facial recognition software, for example, the Colorado database could allow the public movements of every citizen in the state to be identified, tracked, recorded and stored." (2) For this and other reasons to follow, the Colorado Legislature should take two paths with regard to face scanning/recognition. First, abandon any attempt to regulate or legislate a happy face onto the proposed DMV database and simply scrap it, and secondly, ban any routine or general use of facial recognition technology in public places.

Official Function and Original Intent

In Section (IV) (A) of HB 01-1125, the offending Colorado bill, allows for the access and use of DMV images and facial recognition technology to "aid a federal, state or local government agency in carrying out such agency's official function." Well, there are lots of government agencies with a wide variety of "official functions."

The city of Tampa was so enamored with the rollout of the new snooping tool, they decided to keep it around. In Ybor City, an entertainment district of Tampa, it has now become an official function of the police to use facial scanning and recognition software to randomly scan, capture and compare people's faces to a database of wanted felons for engaging in such noxious behavior as strolling down the street. (3) Several city council members who approved the practice now claim they were "tricked" into voting for it; such "I didn't know what I was voting for" confusion seems to be as common a problem at sea level is it is at a mile high. A similar program is underway along the beachfront in Virginia Beach, Virginia (4) and is being considered by other cities.

The rollout of facial recognition into the mainstream of public spaces has already turned on its head the bedrock notion of "Innocent until proven guilty" into "Suspect until cleared by a box of wires." Colorado's facially mapped DMV database as part of a facial recognition platform represents the next step, from random scanning to look for wanted criminals to random scanning to monitor the comings and goings of citizens.

It also threatens to undermine the integrity of police. The honorable profession of "Peace Officer" is already becoming a quaint and antiquated notion. "Drug Warrior" and "Para-Military" are too often descriptive of contemporary law enforcement. Do we also want to add "Omniscient Surveillers"? As Virginia Beach Police Chief A.M. Jacobs puts it, "When people say it's Big Brother watching over you, I like to say it's Big Brother watching out for you." The idea of police as an omniscient force is the antithesis of a free and open society and can only worsen the culture of passivity, rather than self determination and respect for the law, that is pushed by both government and in many news rooms. "Watching out for you" is but a baby step from "Watching over you." Would an "official function" here in Colorado include the scanning and identifying of people peacefully protesting facial scanning in front of the Capitol?

Some years back, the Colorado Department of Revenue was caught selling digitized license photos to Image Data Corporation — at the behest of the Secret Service — for a national "True ID" database. The practice was stopped only after public outcry, but the intent of the database was a bad joke from the beginning. Its official purpose was to fight fraud — a worthy enough cause — but a1997 letter from members of Congress to Image Data praised the program for its "widespread potential." A proprietary Image Data proposal, brought to light through a Freedom of Information Act request pitched the idea to state governments as a "highly effective way of increasing tax revenue." (5)

The lesson from the “True ID” debacle and the Orwellian use of facial recognition technology going on elsewhere is that with government, “intended use” and “official function” are often elastic concepts, open to whatever change the public can be scared, fooled or coerced into accepting. Such “purpose creep” is evident in another DMV practice (albeit one required by the federal government). Coloradans are currently required to hand over their Social Security number before they can get a license, despite the fact that the government at one time promised it would never be used for any purpose other than Social Security. (6)

It’s OK, We’re With the Government

There is an underlying assumption on the part of many that powerful and invasive information systems are acceptable because they are in the hands of government. For those whose power and authority exists solely on the basis of bigger government, the message is clear — being an employee of the state means you are more trustworthy than the public at large. This is the basis for the “If you have nothing to hide, you have nothing to fear” argument being used to justify facial recognition for public scrutiny. But that people may indeed have something to fear is evident from the evolving scandal in Michigan involving the state’s Law Enforcement Information Network (LEIN), a database that utilizes the FBI’s National Crime Information Center, Michigan vehicle registration and driving records, and other databases.

A recent *Detroit Free Press* investigation into abuse of the LEIN has thus far uncovered at least 90 instances of misuse by police officers, dispatchers, security guards and federal agents. The LEIN was used by “trusted” government agents to do favors for friends, stalk women, dig up dirt on an ex-spouse’s new husband, tip off criminal suspects to investigations and, in one case, was used to identify owners of cars with bumper stickers supporting a candidate for sheriff, by a deputy of the incumbent sheriff. (7)

According to the *Detroit Free Press* (8), despite the fact that it is a misdemeanor crime to misuse the system, of the over three dozen police officers found to have abused the system since 1998, only three have faced criminal prosecution. This is mostly because the system is set up to protect government agents who abuse it.

Vagaries in the law differentiate between “official” misuse and general misuse. In other words, if a police officer abused the system for personal reasons or to help a fellow officer, it didn’t rise to a criminal offense. Only if the information was shared with a civilian did the misdemeanor kick in.

Further, the group tasked with overseeing use of the system (consisting of police and Secretary of State officials, judges and prosecutors) was powerless to enforce the law or to punish abuse. Their only authority was to revoke entire agencies’ privileges, which they were understandably loathe to do, and they were required to shred the records of their (non) investigations. Investigation of individual abuses was left to the agency the individual worked for.

Thus, public scrutiny and accountability of government use of a powerful tool of intrusion was made nearly impossible by the very government wielding that tool.
The message is clear: each new tool of intrusion and surveillance represents is also a new tool of potential abuse. Every expansion of the surveillance state will require yet a further expansion of government to watch over the watchers.

The opposition to accountability for facial recognition is already mounting. A recent bill (SB 169) introduced into the California legislature which would have required a warrant prior to scanning someone's face, was defeated in committee with opposition from both law enforcement and the biometrics industry. Senator Debra Bowen, the sponsor of the defeated bill, compared setting up biometric cameras and recording people in public: "[It's] like bugging everyone's phone on a city block and keeping all the tapes on the off chance that someone may have committed a crime, or may commit one in the future." (9)

Lest anyone should think that these such concerns are anti-law enforcement or anti-technology, consider that the Security Industry Association and the CEO of Visionics Corporation (whose facial recognition system is in use in Tampa) have called on Congress to regulate the use of facial recognition technology "To ensure that such systems are not used by police or private corporations to track or compile profiles of innocent citizens." (10) It speaks volumes that those who deal in the technology don't trust their biggest customer (government) to play nice with it.

Feeding the Leviathan

Much of the media attention to Colorado's face-print database has focused on statewide use. It is, after all, the Colorado DMV. But let's not forget about the federal government, which has staked a claim to state DMVs' databases.

Title 18, Sec. 2721 (b) (1) of the U.S. Code allows access to state DMV databases for "Use by any government agency, including any court or law enforcement agency, in carrying out its functions…"

The federal government is many things. In particular it is, as House Majority Leader Dick Armey (R-TX) expressed in a recent speech to the Federalist Society, "The most intrusive force in the lives of Americans." Government is also, more so than credit bureaus and banks, the worst protector of privacy. As Rep. Armey continued, "Government is the biggest privacy offender." For example, this July the Senate Government Affairs Committee released a report of federal agencies' compliance (non-compliance, actually) with government privacy policies: (http://www.senate.gov/%7Ethompson/pr061501.html)

Some of the findings were:

- 300 persistent "cookies on the web sites of 23 different agencies";
- 14 agreements with third parties to share information;
- 42 web bugs;
- 27 agencies in clear violation of their own privacy policies.

Or consider this example of the kind of information the Social Security Administration shares with the IRS as a matter of law, "medical information, including psychological or psychiatric information or lay information used in medical determinations; and information about marital and family relationships and other personal relationships." (11)

Aside from being the single worst privacy offender in America, the federal government also operates, in the words of Michael Hyatt, author of *Invasion of Privacy*, "The single largest surveillance network in the world today." (12) From the FinCEN system, which tracks financial transactions, to the "New Hire" database, which follows us from job to job, to the collecting of everybody's medical histories, the government today quite literally tracks its citizenry from cradle to grave. As author Hyatt continues, "Not only do they have the most resources at their disposal, they have no qualms about using them to collect your personal information — even if it means violating the privacy policies they recommend to the private sector."

The federal government is also the biggest customer for facial recognition technology and is currently funding research into the next generation, The Human ID project, with the goal of identifying people from up to 500 feet away in a variety of lighting and background situations. (13) (Such as on a battlefield or through a dimly lit bedroom window).

As state law can't pre-empt federal law, whatever controls Colorado may put on the face-print database are irrelevant when it comes to the federal government. In effect, Colorado would be creating a face-printed database (with accompanying agency information) of nearly every Coloradan and would have no say in how the most "intrusive force in the lives of Americans" and the biggest customer of face recognition technology uses it.

No Face Scanning/Recognition in Public Places

As noted in the introduction, some uses of facial recognition are pretty unobjectionable and may have a valuable purpose. Face recognition systems in public places, however, do not. The clearest danger is as a political tool: the building and keeping of electronic dossiers on politically unpopular (as opposed to illegal) activities; attending meetings of unpopular groups or clubs; the tracking of attendees of political rallies or protests by out-of-favor activists for out-of-favor causes. Of course, what is out of favor and politically unpopular is open to change, depending on which parties and individuals currently hold political power. One of the more egregious abuses in the Michigan LEIN case took place in Genesee County, where a political appointee of the incumbent sheriff had deputies run the plates of cars sporting bumper stickers in favor of the sheriff's opponent in the upcoming primary race. The practice was discovered only because of an anonymous letter.

The public rollout of facial scanning/recognition technology has the potential to put the enemy files of J. Edgar Hoover to shame.

In his article, "Your Face Is Not A Bar Code: Arguments Against Automatic Face Recognition in Public Places," (14) Philip Agre from the Information Studies Department of the University of California, Los Angeles, makes several other less obvious arguments against face recognition in public:

1. "As the underlying information and communications technologies (digital cameras, image databases, processing power and data communications) become radically cheaper (and more powerful)...new facial image databases will not be hard to construct, with or without the consent of the people whose faces are captured."

2. "The information from face recognition systems is easily combined with information from other technologies…such as 911 location tracking in cell phones…and requires the least cooperation of the individual of all the biometric identification technologies."

3. "It is very hard to provide effective notice of the presence and capabilities of cameras in public places, much less obtain meaningful consent. Travel through many public places, for example, government offices and centralized transportation facilities is hardly a matter of choice for anyone wishing to live in the modern world."

In other words, the faster technology advances, the easier it will be for face scanning/recognition to be expanded and adapted for purposes never intended. It will also become more difficult for adequate public or governmental oversight.

This year, for example, no one in the city government of San Antonio, Texas (outside of the police department) knew that the San Antonio Police had obtained the FaceIt facial recognition software (same as in Tampa) until a newspaper reporter saw them listed as a customer on Visionics Corporation's website. (15) The department purchased the system as part of a mug shot system and claims no plans for population surveillance, but plans can change and the system allows them to start building their own database.

Being the object of some national attention concerning the face-mapping database, Colorado has a unique opportunity to show the rest of the country that public use of face mapping and scanning is not an appropriate function of government in a free and open society. It is not only a bad idea, but its time has not come.

After 9/11

In the aftermath of the terrorist attacks of 9/11, facial recognition is at the top of the list as an anti-terrorism measure. One of the questions being asked is, how much privacy and freedom are we willing to give up for security? A more apt question is what are we going to get in return for what we give up? In England, much has been given up and they have gotten little in return beyond an illusion of safety.

Writing for the *New York Times Magazine* (16), Georgetown University Law Professor Jeffrey Rosen examined Great Britain's use of public monitoring and facial recognition as a terrorism-fighting tool. He found that, far from catching terrorists, biometric surveillance is being used to "enforce social conformity" and "keep punks out of malls." It has also led to new levels of dishonest government.

In the early 90's, the Irish Republican Army set off two large bombs in London's financial district. In response a "Ring of Steel" system of cameras was installed at the entrances of the district. And from there it simply expanded. By 1998, 440 city centers were wired and today there are an estimated 2.5 million surveillance cameras in Britain linked to various biometric databases. According to Rosen, "By one estimate, the average Briton is now photographed by 300 separate cameras in a single day."

What has been the result? According to a City of London press officer, "The technology here is geared up to terrorism, the fact that we're getting ordinary people — burglars stealing cars — as a result of it is sort of a bonus." Have they caught any terrorists? "No, not using this technology."

In the London borough of Newham, things are worse. The monitoring supervisor doesn't know who goes into the database, local police chiefs decide. But it doesn't seem to matter. According to the supervisor, "I'm not in the business of having people arrested, the deterrent value has far exceeded anything you imagine." Such deterrent values include posters exaggerating the capabilities of the system: "The public statements about the efficacy of the Newham facial recognition system bear little relationship to its actual operational capabilities…its effectiveness, perhaps, is based on a lie."

As tools such as face recognition and public scrutiny are debated as anti-terrorist measures, it should be remembered that Americans deserve better than illusions of safety and false promises.

On Sept. 20, Joseph Atick, CEO of Visionics Corporation (maker of Tampa's FaceIt system) met with the Department of Transportation committee tasked with making new airport security recommendations. According to Atick, FaceIt, in conjunction with airport security cameras, could be linked, via the Internet, to a federal monitoring station and could alert officials to a match within seconds.

He also added that virtually any camera, anywhere could be linked to the system. (17) As can a "wide network of intelligence databases." (18)

The point here is two-fold. First, that facial recognition is a potentially valuable tool for airport security and anti-terrorism. And second, if Mr. Atick is correct, the notion that the Colorado database "could allow the public movements of every citizen in the state to be identified, tracked, recorded and stored" is real and could be done from a "federal monitoring station."

The heart of the matter is what, or rather, who goes into the databases.

Visionics Corporation has issued a White Paper detailing the elements of their proposed anti-terrorist system. (19) In it they explain just what these databases should contain, "Modify the boarding process to require an instantaneous terrorist background check on each passenger upon check-in and boarding by searching facial images against intelligence databases of terrorists and their affiliates."

It would be entirely appropriate for the U.S. intelligence and counter-terrorist forces to use their reach and resources to put together just such a database, as it seems certain that some sort of biometrics platform will be employed at airports. The use of existing police and surveillance powers to bring together the scattered knowledge of terrorists operating in and out of the U.S. into a more seamless system seems sorely needed. But this should not be used as a reason to push ahead with the DMV faceprint database.

Moreover, Colorado should be seeking assurances that the federal government is not planning to use its own "official function" access to the DMV data to use the existing digital photos and associated information to make their own "faceprint" database.

Terrorists and their affiliates, yes, definitely facemap them. But not all licensed Coloradans just because the technology exists.

The Great Britain experience also brings up the question of efficacy. Will mapping the faces of license applicants stop the issuance of multiple licenses to the same person using the same picture?

In his article, Jeffrey Rosen points out that in a recent documentary about CCTV, actor John Cleese fooled a Visionics face recognition system by wearing a fake beard and earrings. (16) But it is not just British comedians who question the reliability of facial recognition.

Last year, according to Jim Wayman, director of the National Biometric Test Center at San Jose State University, a DOD-funded test of commercially available face recognition systems failed a third of the time and adds there is a major problem with false positives, where a match is signaled when in fact there is none. (20) The Tampa Super Bowl experiment reportedly made 19 matches against a database of known criminals, but according to the *Wall Street Journal*, an unknown number of those matches were false. According to a Tampa Detective who worked on the test, “I looked at some of those side-by-side pictures (a picture of the football fan next to the picture from the database) and they weren’t the same person.” (20)

According to the experts, facial recognition works best in tightly controlled, well-lit situations, such as the taking of drivers’ license photos. But even here, the best just isn’t very good. According to Anil Jain, a Computer Vision Professor at Michigan State University, the system can be fooled by beards, by different hairstyles, and wearing glasses. (20) Similarly, Julian Ashbourn, author of “Advanced Identity Verification” claims the technology can be fooled by lighting and the angle of the face. (21)

A facial recognition study by the National Institute of Standards and Technology (22) found that photos of the same person taken 1 ½ years apart had a false rejection rate of 43%. Professor Jain also claims that the aging process can easily fool the software.

In other words, while the Colorado plan may result in catching teenagers seeking fake ID’s to party with, those willing to change their appearance or who have aged may have little to worry about.

As with most technology, face recognition will probably improve over time and, as Professor Takeo Kanade of Carnegie Mellon University told the *Wall Street Journal*, after substantial federal money has been committed to make that happen. But as we all know, we have a big problem right now.

Technology can be a valuable too. It can also be a crutch. As has been noted by some in the intelligence community, part of the problem over the years, brought painfully to light, has been a dependence on technology and electronic surveillance at the expense of human intelligence: eyes and ears on the ground. Some of the pieces put together as to the obtaining of ID’s by the terrorists of 9/11 point to document fraud and graft, such as the use of bribery to obtain affidavits and pre-notarized forms (23) and the theft of foreign identities and forged INS documents (such as the form I-94). It is not clear that face mapping is the answer to such problems. Nor does it address other such issues as computer-generated fake ID’s, or licenses made from stolen DMV materials (scandalously common). It would be a tragedy to find a false sense of security in an unproven and experimental hi-tech system while the bad guys use low-tech means to beat the system.

State agencies have limited resources. It seems that what is needed is not more uncertain technology, but more real-life investigators with adequate resources to protect the physical security of DMV materials and catch the forgers, frauds and thieves before they can acquire bogus but solid-looking original ID’s. Once they have that, they have little to fear from having their faces mapped.

Endnotes

(1) Denver Post, July 15, 2001 “Approval of facial mapping reviewed”
(2) Joint Statement of House Majority Leader Dick Armey and the American Civil Liberties Union
(3) News4Jax, Don’t smile, you’re on candid camera 08/09/2001
(4) The Virginia-Pilot, July 27, 2001 “Beach police win grant to scan faces”
(5) Wired News, March 14, 2001, “Smile, your on scan camera”
(6) “Short history of the social security number” Computer Professionals for Social Responsibility, www.cpsr.org
(7) Detroit Free Press 07/31/2001 “Cops tap database to harass, intimidate”
(8) Detroit Free Press 08/01/2001 “Penalties uneven for data misuse”
(9) (10) Wired News, July 31, 2001, “Face scanners turn lens on selves”
(11) CFR, Title 20, Chap.111, Subpart C, sec.401.120
(12) Michael Hyatt “Your privacy for sale” moreprivacy.com Sept, 10, 2001
(13) Wired News, Sep. 7, 1999, “Smile for the U.S. Secret Service”
(14) http://dlis.gseis.ucla.wdu/peoplw/pagre/bar-code.html
(15) San Antonio Lightning, August 28, 2001, “S.A. Police confirm they have face recognition software”
(16) The New York Times Magazine, October 7, 2001, “A Cautionary Tale for a New Age of Surveillance”
(17) Washington Post, Sept.24, 2001, “Facial recognition system considered for U.S. airports”
(18)(19) “Protecting civilization from the faces of terror: A primer on the role facial recognition technology can play in improving airport security” http://www.visionics.com/newsroom/downloads/whitepaper/counterterrorism.pdf
(20) Wall Street Journal, Technology Journal, B11, Sept. 27, 2001, Face Recognition Technology Questioned”
(21) http://homepage.ntlworld.com/author.htm
(22) http://dodcounterdrug.com/facialrecognition/DLs/feret7.pdf
(23) Yahoo Daily News, Oct. 9, 2001, “Hijackers’ ID’s Prompt Scrutiny”