Biometric Facial Recognition Software:

How the Law Should Treat Machines as Witnesses

Stephen Andrew Mosca

Table of Contents

Table of Authorities

Cases

Statutes

Other Authorities

DAVID L. FAIGMAN, DAVID H. KAYE, MICHAEL J. SAKS, JOSEPH SANDERS, SCIENCE IN THE LAW; FORENSIC SCIENCE ISSUES 24 (West group, St. Paul, Minn. 2002) 11
Declan McCullah, *Call it Super Bowl Face Scan I*, Wired News, at http://www.wired.com/news/politics/0,1283,41571,00.html 36
E. Martin Estrada, *Criminalizing Silence: Hiibel and the Continuing Expansion of the Terry Doctrine*, 49 St. Louis U. L.J. 279 (2005) 27
http://aclu.org//privacy/spying/14874prs20030902.html 22
http://www.face-rec.org/vendors 12
http://www.findbiometrics, com/Pages/dace_articles/face_2.html 21
http://www.frvt.org 13
http://www.frvt.org/FERET/default.htm 14
http://www.FRVT.org/FRVT2002/default.htm 16
http://www.FRVT.org/FRVT2006/default.htm 16
http://www.itl.nist.gov/lab/pub/newsmay03.htm 12
http://www.wired.com/news/culture/0,1284,56878,00.html 21
http://xml.coverpages.org/FRVT-2002.html 17
http:www.FRVT.org/FRVT2000/default.htm 15
Jay Soloman, *Investing in Intelligence; Spy Agencies Seek Innovation Through Venture-Capital Firm*, The Wall Street Journal, September 12, 2005 13
Jeffery H. Reiman, *Driving to the Panopticon: A Philisophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, 11 Santa Clara Computer & High tech. L. J. 27 33
JOHN D. WOODWARD, JR., CHRISTOPHER HORN, JULIUS GATUNE, ARYN THOMAS, BIOMETRICS. A LOOK AT FACIAL RECOGNITION (Rand, Santa Monica, CA 2003) 10
JOHN D. WOODWARD, JR., CHRISTOPHER HORN, JULIUS GATUNE, ARYN THOMAS, BIOMETRICS. A LOOK AT FACIAL RECOGNITION (Rand, Santa Monica, CA 2003) 11
JOHN STUART MILL, ON LIBERTY (Hackett Publishing Company, 1978 33
Joyce Purnick, *Speak Out. The Police Are All Ears*, N.Y. Times, April 21, 2003 37
JULIAN ASHBOURN, BIOMETRICS. ADVANCED IDENTITY VERIFICATION. THE COMPLETE GUIDE (Springer-Verlag London Limited 2000) 10
Katherine Shrader, *The Pentagon Wants to Talk to You – On the Sly*, Associated Press, October 18, 2005 40
Lee Gomes, *Videotape Can Help ID Terrorists, but Humans Must Still Do Scanning*, The Wall Street Journal, July 13, 2005 19
Lee Gomes, *Videotape Can help ID Terrorists, but Humans Must Still Do the Scanning,* The Wall Street Journal, July 18, 2005 12
Linda E. Fisher, *Guilt by Expressive Association: Political Profiling, Surveillance and The Privacy of Groups*, 46 Ariz. L. Rev. 621 36
P. JONATHON PHILLIPS, PATRICK GROTHER, ROSS J. MICHEALS, DUANE M. BLACKBURN, ELHAM TABASSI, MIKE BONE, FACE RECOGNITION VENDOR TEST, OVERVIEW AND SUMMARY, March, 2003 (DARPA, Arlington, VA) at http://www.frvt.org/DLs/FRVT_2002_Overview_and_Summary.pdf 17
Quentin Burrows, *Scowl Because You're on Candid Camera; Privacy and Video Surveillance*, 31 Val. U. L. Rev. 1079 (1997) 36
RICHARD WASSERSTROM, PRIVACY: SOME ARGUMENTS AND ASSUMPTIONS, IN PHILOSOPHICAL DIMENSIONS OF PRIVACY (Ferdinand Schoeman, ed., 1984). 32

Treatises

Constitutional Provisions

Introduction

It is the conventional wisdom that the "[L]aw lags science; it does not lead it."[1] However, it has also been asserted that the mere specter of science may hoodwink jurors into granting validity to theories and processes that have yet to obtain the legitimacy borne of true scientific rigor.[2] Facial recognition is a technology that promises to change the nature of life in a free society. For this reason, it would be wise to consider the potential implications of facial recognition technology before it becomes deeply rooted within the future social and legal fabric of our society.

Politics, Economics, and Technology

Political circumstances have often provided a motive for a state's developmental path. There is a symbiotic relationship between any contemporary period's politics, economics, and the development of technology. During the Second World War, fascism required the West to adapt its highly developed industrial infrastructure to the mass production of conventional weapons and relatively high precision targeting systems. Ultimately, the effort produced the technology to develop nuclear weapons as well. Economically, the success of liberating Western Europe and Japan provided an immediate market for the export of infrastructure rebuilding products and services. Once developed, that market matured into a diversified production base and liberalized capital markets world wide.[3]

During the Cold War, Communism arose with the advent of electronic computing technology. This technology was used to design and build weapons that could project great

[1] Rosen v. Ciba-Geigy, 78 F.3d 316, 319 C.A. 7 (Ill.) 1996.
[2] Logerquist v. McVey, 196 Ariz. 470, 481 (Ariz. 2000).(asserting that juries have been fooled by "junk science").
[3] RONALD W. COX & DANIEL SKIDMORE-HESS, U.S. POLITICS & THE GLOBAL ECONOMY. CORPORATE POWER, CONSERVATIVE SHIFT 12 (Lynne Rienner Publishers. Boulder, CO. 1999).

force at a distance, using precision guided nuclear delivery systems. Electronics were also employed in sophisticated communications and communication interception and jamming systems. Economically, the United States sought to liberalize trade policy, thereby giving global partners a market based incentive to stem the spread of communism.[4]

More recently, and particularly in the post September 11, 2001 period, politics has again changed the face of technological development priorities. Terrorism employs stateless actors using asymmetrical tactics to destabilize the global market system of liberalized Western democracies. Free trade's open borders provide the means for individual terrorist cells to infiltrate and unleash surprise attacks within the target nation with little or no advanced warning. Economically, a service economy built upon intellectual capital and expressed digitally requires the suppression of these attacks for continued growth.

Counter-terrorism requires that domestic intelligence locate for interception those who plan, recruit, and deploy terrorist tactics. Thus, surveillance systems that are small, unobtrusive, and linked to powerful computers are needed. These systems sift through and fuse the reams of data that a modern society generates in order to identify, locate, and track terrorist suspects before they can wreak economic havoc.

Facial recognition technology is uniquely suited to accomplish the counter-terror mission. The deployment of facial recognition systems at ports of entry is one application that makes intuitive sense. The location and identification of possible terrorist actors by tracking their movements through city centers or in relation to the routes and landmarks they choose to visit also has practical application. This latter use implicates issues that affect domestic society in ways that are as yet unexplored.

[4] Id. at 107.

This article will examine the current state-of-the-art in the underlying science of facial recognition technology as applied to the use of government placed cameras in public places. It will also consider how the legal system may treat the continuing evolution of privacy jurisprudence in light of this emerging technology.

Science and the Law

The role of science in the law is involved primarily with evidentiary issues. The role of forensic evidence is to individualize suspects. This refers to the desire to tie a piece of evidence, be it a fingerprint, voice or handwriting sample, blood or other biological sample, to one person to the exclusion of all others.[5] With the advent of computer technology, mass-biometric measurements have gained new importance in the field of law enforcement and criminal justice. Once a painstaking individual effort, the automated matching of a biometric sample to an individual by comparing the sample to a database composed of thousands or even millions of known samples is now commonplace.[6]

Legally, the chief concern regarding evidence is the desire for it to be reliable.[7] When a technology is used as a method to ensure the reliability of evidence, it is important to understand the underlying science employed. For this task, the law permits the testimony of experts to inform the jury. However, the decision as to what is legally reliable is left not to the scientists or technological experts themselves but to the sole discretion of the trial judge.[8] In fact, a trial court has complete discretion over whether expert testimony is admissible as to its reliability and relevance, not only for scientific knowledge but also for "technical" and "other

[5] DAVID L. FAIGMAN, DAVID H. KAYE, MICHAEL J. SAKS, JOSEPH SANDERS, SCIENCE IN THE LAW; FORENSIC SCIENCE ISSUES 9 (West group, St. Paul, Minn. 2002).
[6] Id. at 101. (AFIS systems screen millions of fingerprints and efficiently selects candidates for comparison.)
[7] U.S. v. Scheffer, 118 S. Ct. 1261, 1265 (1998) ("Indeed, the exclusion of unreliable evidence is a principal objective of many evidentiary rules.").

specialized" knowledge as well.[9] This is an expansion of the factors articulated in *Daubert,* created to govern the admission of purely scientific evidence and expert opinion.[10] Under *Frye v. United States*, the question is narrowed to whether the methods are generally accepted within the relevant scientific community.[11] Obviously, there must be good information available from which a trial judge may become educated if they are to be effective gatekeepers of expert testimony.

Additionally, such evidence must be deemed by a trial judge to merely be of assistance to the triers of fact in reaching a decision or conclusion. Since there is no need for expert testimony to be exclusive of all doubt, it is especially important that reliability, and thus the quality of impact, upon the opinion of a layperson be established both accurately and fairly.

Once a court takes judicial notice of the reliability of a science or technology, it becomes extremely difficult for an accused to refute such evidence.[12] Justice can hardly be done when something considered reliable has never actually been demonstrated or proven to be accurate.

One tautological frustration standing in the way of corrective measures is known as the "guild" test. The guild test asserts that only those practiced in performing the procedure or technology in question are in a proper position to critique it, thus assigning only admitted adherents as potential critics. This is vividly illustrated in *People v. Hyatt*.[13] In *Hyatt*, Dr. Cole, a scholar with years of academic research into the history underlying fingerprint analysis, was castigated for his opinions because he himself was not an expert in the practical aspects of

---

[8] Id. at 1171 (holding that reasonable measures of expert's reliability in a particular case is a matter that the law grants the trial judge broad latitude to determine.)

[9] Kumho Tire Co., Ltd. v. Carmichael, 119 S. Ct. 1167, 1170 (1999) . ("We conclude that Daubert's general holding—setting forth the trial judge's general 'gatekeeping' obligation—applies not only to testimony based on 'scientific' knowledge, but also to testimony based on 'technical' and 'other specialized' knowledge.")

[10] *See generally* Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993)

[11] 293 F. 1013 (D.C. Cir. 1923).

[12] Kumho Tire Co., Ltd. v. Carmichael, 119 S. Ct. 1167, 1170 (1999) ("A court of appeals must apply an abuse-of-discretion standard when it reviews a trial court's decision to admit or exclude expert testimony.")

latent fingerprint collection and comparison. The court held that "Dr. Cole's proposed attack on the scientific underpinning of fingerprint identification is more in the nature of the roll of an advocate or historian…," therefore, "his testimony would neither be relevant to the issues…nor assist the jurors who as triers of fact might be in need of specialized information."[14]

The court maliciously classified Dr. Cole's testimony as to the historical lack of scientific validation underpinning traditional fingerprint reliability as "junk science."[15] With this in mind, it is especially important to establish at the outset the standards and validity of any new technology that is likely to become prevalent in our criminal justice system as well as in our courtrooms.

Modern Biometrics

Biometric technologies are those that seek to recognize or identify an individual using distinguishing biological traits. While the method is ancient, modern definitions are distinguished by inclusion of a technological element that automates the process. A modern and expansive definition is "any automatically measurable, robust and distinctive physical characteristic or personal trait that can be used to identify an individual."[16] In this definition, "measurable" means that the characteristic or trait "can be easily presented to a sensor, located by it, and converted into a quantifiable, digital format."[17] "Robust" refers to the extent to which the characteristic or trait is subject to significant change over time.[18] "Distinctive" is a measure of the variations in the biometric pattern among the general population.[19] Any

---

[13] People v. Hyatt, 2001 WL 1750613 (N.Y. Sup. Ct.)
[14] Id. at 2786.
[15] Id.
[16] JOHN D. WOODWARD, JR., CHRISTOPHER HORN, JULIUS GATUNE, ARYN THOMAS, BIOMETRICS. A LOOK AT FACIAL RECOGNITION 1 (Rand, Santa Monica, CA 2003).
[17] Id.
[18] Id.
[19] Id.

automated system used to identify a person by their facial features must be evaluated in terms of these various definitions to determine its ability to perform adequately.

The Distinction: Identification and Verification

The concern here is with individualization, or identification, and not verification techniques. Verification is currently the more widely used methodology in which the enrolled user has a template that is firmly associated with that user residing on the system. When a transaction is undertaken the user calls up this particular template, usually by using a personal identification number (PIN), and the machine takes a live biometric sample. The task is to then compare and match the two records. "The user is in effect claiming an identity by inputting the reference number and the system is subsequently verifying that the claim is genuine or otherwise, according to the matching criteria setup within the system."[20]

In identification mode, a system is attempting something quite different. There is still a database of templates, but now the sample biometric has to be compared to all of them. This is not as straightforward as it may sound; what if none of the templates within the database match the submitted sample particularly well? What if there are several templates within the database that qualify as a potential match? The key to whether a system can perform well in this mode of operation lies in the confidence level of the matching process. Confidence levels must be established through testing sufficient to establish a meaningful statistical calculation of error. Meaningful error rate calculation is often the most scientific aspect of biometric evidence integrity and, typically, the least well established.[21]

---

[20] JULIAN ASHBOURN, BIOMETRICS. ADVANCED IDENTITY VERIFICATION. THE COMPLETE GUIDE (Springer-Verlag London Limited 2000).

[21] DAVID L. FAIGMAN, DAVID H. KAYE, MICHAEL J. SAKS, JOSEPH SANDERS, SCIENCE IN THE LAW; FORENSIC SCIENCE ISSUES 24 (West group, St. Paul, Minn. 2002). ("Statistical rates of a technique's success in identification may be established through rigorous testing. Such testing will produce data with a high degree of variation among attributes, then, when a 'match' is observed, the probability that the match is coincidental rather than reflecting a

Facial Recognition Technology Development

Facial recognition records and compares the spatial geometry of distinguishing features of the face or can be based on an image mode of recognition. "Different vendors use different methods of facial recognition, however, all focus on measures of key features of the face."[22] The different methods used by various vendors are difficult to quantify specifically because all such products are proprietary in nature.[23] Various claims made by vendors as to the capability of their particular system are also difficult to evaluate.[24] Indeed, after the London bombings in the summer of 2005, many vendors tried to capitalize on the publicity. Citing London's extensive CCTV camera system used to identify the individuals responsible for the bombings, many sent out press releases touting advances in their particular systems without any testable basis for their expansive claims.[25] One may rightly wonder, then, how the government could decide on the effectiveness of a system prior to its deployment.

In order to evaluate both commercial and government developed systems the government has instituted a rigorous testing policy. The Commerce Department's National Institute of

---

shared source will be very small. Forensic sciences that have such data can actually calculate the probability of a coincidental match and report that probability to the judge and jury. Moreover, since the basis of all forensic identification is probability theory, examiners can really assert a conclusion of an 'identification to the exclusion of all others in the world,' but at best can only assert a very small (objective or subjective) probability of a coincidental match. Forensic individualization sciences that lack actual data, which is most of them, have no choice but to either intuitively estimate those underlying probabilities and calculate the coincidental match probability from those subjective probabilities, or simply to assume the conclusion of a miniscule probability of a coincidental match (and in fact they do the latter).)

[22] JOHN D. WOODWARD, JR., CHRISTOPHER HORN, JULIUS GATUNE, ARYN THOMAS, BIOMETRICS. A LOOK AT FACIAL RECOGNITION 3 (Rand, Santa Monica, CA 2003).

[23] INTELLIGENT BIOMETRIC TECHNIQUES IN FINGERPRINT AND FACE RECOGNITION (L.C. Jain, U. Halici, I. Hayashi, S.B. Lee, S. Tsutsui, eds., CRC Press, Boca Raton, FL. 1999) (Methods under development and supported by mathematical modeling include multi-modal facial information, space-variant sampling, Eigenfaces, deformable templates and active shape models, receptive field-based approaches, Gaussian receptive fields, natural basis functions, Laplacian/difference of Gaussians, Gabor wavelets, hidden Markov models, and convolutional networks.)

[24] *At* http://www.face-rec.org/vendors (accessed 10/24/05). Vendors listed include: A4Vision, Inc., AcSys Biometrics, Corp., Animetrics, Inc., C-VIS Computer Vision und Automation, GmbH., Cognitec Systems, GmbH., Cybula, Ltd., DreamMirh, Co., Ltd., Geometrix, Inc., Iconquest, Identix, Inc., Imagis technologies, Inc., Neven Vision, Inc., Takumi Vision Technologies, Inc., Viisage, Visionsphere Technologies, Inc.)

Standards and Technology (NIST), in conjunction with the Defense Advanced Research Projects Agency (DARPA) and the Department of Defense's Counter-Drug Technology Development Program Office, have developed the FRVT (Face Recognition Vendor Test).[26] The FRVT was designed to be double blind, i.e.; neither the identification of a particular vendor is known to the testers and the vendors do not know what the test consists of in terms of methodology. This is intended to prevent selection of a preferred vendor as well as to prevent a vendor from tweaking their system to better match desirable characteristics of performance under test conditions.[27] But already, conflicts of interest are apparent.

"The Federal Bureau of investigation (FBI) and the Pentagon's Defense Intelligence Agency (DIA) are beginning to invest in start-up companies, following U.S. intelligence agencies in using taxpayer money to spur development of high-technology products and services by U.S. entrepreneurs."[28] The concern is that the government tracks and publishes returns on its investments, perhaps leading to pressures to show good performance. Additionally, one recipient of government funds for private product development stated, "its relationship with [the Central Intelligence Agency (CIA) established venture-capital firm In-Q-Tel] has given the company unique access to other potential government clients, unusual for a start-up."[29] Somehow, integrity in the testing and acquisition process must me maintained.

The importance of testing and the validation of the test methods cannot be overstated. While the methodology underlying all of the facial recognition technologies is mathematical in nature, this is not, in itself, evidence of a scientific basis. Science is a process that seeks to

---

[25] *See* Lee Gomes, *Videotape Can help ID Terrorists, but Humans Must Still Do the Scanning,* The Wall Street Journal, July 18, 2005 at B1.
[26] *At* http://www.itl.nist.gov/lab/pub/newsmay03.htm (Accessed 10/25/05).
[27] *See generally* http://www.frvt.org (accessed 10/15/05).
[28] Jay Soloman, *Investing in Intelligence; Spy Agencies Seek Innovation Through Venture-Capital Firm*, The Wall Street Journal, September 12, 2005 at A4.
[29] Id.

offer a theory or hypothesis and then to construct an experiment that either confirms or refutes that theory on repeatable basis. Experiments must be constructed carefully to ensure that they confirm or refute the theory correctly and completely. In the area of facial recognition technology, mathematics are a tool only and cannot confirm the accuracy of the algorithms designed to generate the end result. It is the testing regime that embodies the scientific method.

Evolution of Testing Methodology

Like most compute-intensive technologies, facial recognition has progressed apace the improvements in computing resources available to process the data. Initial tests, called FERET (Facial Recognition Technology program), were held in 1994.[30] Subsequent FERET tests were held in 1995 and 1996.[31] "The FERET program introduced evaluations to the face recognition community and helped advance face recognition from its infancy to the prototype system stage."[32] Early FERET tests used standard databases composed of a consistent physical setup using a controlled environment.[33]

> The FERET database was collected in 15 sessions between August 1993 and July 1996. The database contains 1564 sets of images for a total of 14,126 images that includes 1199 individuals and 365 duplicate sets of images. A duplicate set is a second set of images of a person already in the database and was usually taken on a different day. For some individuals, over two years had elapsed between their first and last sittings, with some subjects being photographed multiple times. This time lapse was important because it enabled researchers to study, for the first time, changes in a subject's appearance that occur over a year.[34]

The independently administered FERET tests allowed for a direct quantitative assessment of the relative strengths and weaknesses of different approaches. This provided the facial

[30] *At* http://www.frvt.org (accessed November 9, 2005).
[31] Id.
[32] Id.
[33] *At* http://www.frvt.org/FERET/default.htm (accessed November 9, 2005).
[34] Id.

recognition vendor community with an unbiased and open evaluation of the important technical problems that needed to be addressed.

Each successive FERET test was designed to evaluate the progress vendors were making in improvement of performance from the earlier tests. The final test had systems check over 12.6 million images and used subjects that were photographed in different lighting conditions and at various ages.[35] Clearly, the early work done in the FERET program was instrumental to the efficient launch of the technology as well as its development. Much of the technology funded by the government during this period was seeded into the commercial market of system developers. The FERET test series was officially discontinued in 1997.

In the year 2000, 2002, and planned for 2006, are evaluations built upon the early FERET tests known as the FRVT (Facial Recognition Vendor Test) test series. These tests are designed to evaluate what are considered fully functional commercial systems as opposed to FERET's prototype systems. The 2000 FRVT was primarily an evaluation of early commercial systems and measured progress achieved since the final FERET test.[36]

FRVT 2000 consisted of two components: the Recognition Performance Test and the Product Usability Test. The goal of the Recognition Performance Test was to compare competing techniques. All systems were tested on a standardized database using the same images which allowed for comparison of the core technology. The product usability test examined access control.[37]

[35] Id.
[36] *At* http://www.FRVT.org (accessed November 9, 2005).
[37] *At* http:www.FRVT.org/FRVT2000/default.htm (accessed November 9, 2005).

"FRVT 2002 was designed to measure technical progress since 2000, to evaluate performance on real-life large-scale databases, and to introduce new experiments to help understand face recognition performance better."[38]

> FRVT 2002 consisted of two tests: the High Computational Intensity (HCInt) Test and the Medium Computational Intensity (MCInt) Test. Both tests required the systems to be fully automatic, and manual intervention was not allowed. Participants could sign up to take either or both tests.
> The High Computational Intensity (HCInt) Test was designed to test state-of-the-art systems on extremely challenging real-world images. These were full-face still frontal images. This test compared still database images against still images of an unknown person. The HCInt required participants to process a set of approximately 121,000 images, and match all possible pairs of images from the 121,000-image set. This required performing 15 billion matches in 242 hours. The results from the HCInt measure [sic] performance of face recognitions systems on large databases, examine the effect of database size on performance and estimate [sic] variability in system performance.
> The Medium Computational Intensity (MCInt) Test consisted of two separate parts: still and video. MCInt was designed to provide an understanding of a participant's capability to perform face recognition tasks with several different formats of imagery (still and video) under varying conditions. The still portion of the MCInt is similar to the FERET and FRVT 2000 evaluations. It compared a database of still images against still images of unknown people. The still portion of the MCInt was designed to measure performance on different categories of images. Examples of different effects that were measured were time between images, changes in illumination, and variation in pose. The video portion was designed to provide an initial assessment of whether or not video helps increase face recognition performance. This portion used video style imagery that was extracted from digital video sequences.[39]

The FRVT2006 is scheduled for January, 2006. It includes all the goals of past tests plus high resolution imagery (5-6 mega-pixels), 3D facial scans, multi-sample still facial imagery, and pre-processing algorithms that compensate for pose and illumination. FVRT2006 will use data not previously used in terms of database and test parameters and be conducted by NIST.[40]

Currently ongoing is the Facial Recognition Grand Challenge (FRGT). The FRGC is a separate algorithm development project designed to promote and advance face recognition technology that supports existing face recognition efforts in the U.S. Government. One of the

[38] *At* http://www.FRVT.org (accessed November 9, 2005).
[39] *At* http://www.FRVT.org/FRVT2002/default.htm (accessed November 9, 2005).
[40] *At* http://www.FRVT.org/FRVT2006/default.htm (accessed November 9, 2005).

objectives of the FRGC is to develop face recognition algorithms capable of performance an order of magnitude better than FRVT 2002.[41]

While the FRVT 2006 is being conducted by the National Institute of Standards and Technology (NIST), it is jointly sponsored by five other U.S. Government agencies who share NIST's interest in measuring the improvements in face recognition technologies. They are: the FBI, the Intelligence Technology Innovation Center, the National Institute of Justice, the Technical Support Working Group, and the U.S. Department of Homeland Security, Science & Technology.[42]

Results of these tests show rapid improvements in the technology, though none seem ready for operational deployment. Among factors considered, researchers evaluated demographic factors affecting the ability to recognize faces. "These results show that males are easier to identify than females, and older people are easier to recognize than younger people. The study also found significant differences in matching abilities depending on whether the images were taken indoors or outdoors."[43] Indoor images taken under controlled lighting were easier to evaluate accurately.

FRVT2002 produced mixed results and "raised more questions than it answered."[44] At best, systems were able to make accurate matches 85% of the time and that figure decreased with increases in database size and reduced time to process images.[45] Hopefully, with an error rate of 15% during optimal test conditions, real world deployment is not imminent.

---

[41] Id.
[42] Id.
[43] *At* http://xml.coverpages.org/FRVT-2002.html (accessed November 9, 2005).
[44] P. JONATHON PHILLIPS, PATRICK GROTHER, ROSS J. MICHEALS, DUANE M. BLACKBURN, ELHAM TABASSI, MIKE BONE, FACE RECOGNITION VENDOR TEST, OVERVIEW AND SUMMARY, March, 2003 (DARPA, Arlington, VA) at http://www.frvt.org/DLs/FRVT_2002_Overview_and_Summary.pdf (accessed November 9, 2005).
[45] Id.

Recently, the State Department used NIST data to determine effective technologies for use in new international passports. Facial recognition was disqualified as a candidate technology because "NIST tests showed that facial recognition has an accuracy rate of about 95%."[46] Perhaps the gain in the NIST accuracy numbers reflects progress made since the published FRVT 2002 results. Further comments included the difficulty of achieving good results under uncontrolled conditions, a theme made evident by the published test results.[47]

Digital photographs are a part of the new passport format however, meaning that a controlled image is now a part of each passport file created. Such images will make it much easier for next-generation validation systems to do their job. Images will also be available, from passport and drivers' license photos, to add to any database used to seek an individual's location or movements whenever real-time facial recognition technology is successfully deployed in the future.

Trial Deployments

There are many instances of real-world deployment of surveillance technology as well as facial recognition systems. The deployments of automated technology may be considered experimental in nature, and do not yet rise to the level of investigative or probative usefulness as evidence. Each level of use implicates different legal factors for analysis and consideration. In most cases to date, humans monitor cameras mounted in urban areas or have those images recorded for later review. In select cases, automated systems were tried out in real time, with software algorithms attempting to match passersby with a database of known criminals. Results of these trials are instructive.

---

[46] *Testing the Technology*, The Wall Street Journal, October 17, 2005. http://online.wsj.com/article/SB112609197711133888.html. (accessed October 18, 2005).
[47] Id.

An early use of technology to recognize faces in the criminal context occurred in California over 15 years ago. "In 1988, the Lakewood Division of the Los Angeles County Sheriff's Department installed a system that can take a composite drawing or a video image of a suspect caught committing a crime and search that picture with the database of digitized mug shots on file."[48] Since that time, several domestic deployments have occurred with each using a more advanced version of hardware and software.

Perhaps the largest deployment of closed circuit television cameras (CCTV) in a Western democratic nation exists in the United Kingdom. "In 1997 and 1998, bids established 2,298 new cameras, and trade magazines calculated that the UK CCTV market was valued at over $490 million annually. British citizens can expect to be caught on CCTV 500 times per week and have personal details stored on 300 corporate or government databases."[49]

The UK technology "played a central role in the identification of the 'ordinary British lads' believed to be responsible for London's July 7 bus and subway bombings."[50] London's central monitoring location records video feeds from the various cameras located around the city for later review. Human beings must search the tapes manually to locate suspects after an activity or suspicion arouses their interest.[51] While this is not automated facial recognition, the sheer scope of deployed cameras in the UK gives pause.

If this network of surveillance cameras were linked to a workable facial recognition engine, a fully operational tracking and surveillance system would be in place with the flip of a switch. In the UK, currently operating under the rights-based law of the European Court of

---

[48] *See* Stephen Coleman, Biometrics: Solving Cases of Mistaken Identity and More, F.B.I. L. Enforcement Bull., June 1, 2000 at 13.
[49] *See* Alan Beckly, *The Future of Privacy in Law Enforcement: The United Kingdom's Experience*, FBI Law Enforcement Bulletin – September 2004, Volume 73, Number 9 at 17. http://www.fbi.gov/publications/leb/2004/sept2004/sept04leb.htm (Accessed September 10, 2005).
[50] Lee Gomes, *Videotape Can Help ID Terrorists, but Humans Must Still Do Scanning*, The Wall Street Journal, July 13, 2005, at B1.

Human Rights, public authorities must not infringe on the rights of citizens without legitimate cause.[52] Citizens in the UK do not seem to be overly concerned though concerns do exist, even in the UK, when police departments use community volunteers to view CCTV monitors in a cost costing initiative.[53] Additionally, the technical capability of the UK camera system may not be at the level needed for accurate, automated facial recognition systems. However, once the public accepts the presence of cameras in principle, there is nothing to indicate that higher resolution or stereo image system upgrades, suitable for creating more accurate 3D images of subjects, would evoke protest where current technology does not.

In the United States, deployments of automated systems against criminal targets have not been very successful. Private and localized state use is growing, none-the-less:

> Major casinos now use the technology to spot card counters at blackjack tables. Several states are using face-recognition systems to check for individuals who have obtained multiple driver's [sic] licenses by lying about their identity. Pinellas County, Florida, recently began deploying the system in police cars so officers can check the people they stop against a database of photographs without having to go back to the office.[54]

The private market for facial recognition technology in the United States was estimated at $144 million in 2004, a figure sure to grow in the future.[55] Revenues are estimated to climb to more than $800 million by 2008, according to International biometrics.[56]

Government sponsored research in the United States has been varied. Both Virginia Beach, Virginia and Tampa, Florida have seen trial use of facial recognition technology. Both trials are considered failures. Baltimore, Maryland has installed a large surveillance network,

---

[51] Id.
[52] See Alan Beckly, *The Future of Privacy in Law Enforcement: The United Kingdom's Experience*, FBI Law Enforcement Bulletin – September 2004, Volume 73, Number 9 at 17.
[53] Id.
[54] *See* Barnaby J. Feder, *Technology Strains to Find Menace in the Crowd*, The New York Times, May 31, 2004 at C2.
[55] Id.
[56] Id.

and numerous airport deployments, generally for access control, i.e.; verification mode, have been attempted. None of these efforts has yielded positive published results.

In 2001, Tampa hosted the Super Bowl. A facial recognition system scanned the 100,000 attendees against a database of suspects in search of potential terrorists. The system picked out 19 people with criminal records, but none were among those being sought by authorities.[57] Authorities would not disclose who was in their database, but police indicated afterwards that of the 19 flagged individuals, "some were false alarms" and no one flagged was more than a "petty criminal."[58] The effort was considered unsuccessful and was dropped from consideration the following year.[59]

Also in 2001, the Virginia Department of Criminal Justice Services gave a $150,000 grant to the City of Virginia Beach to help the city obtain face recognition cameras to look for criminal suspects and missing children.[60] After a year of deployment, not a single person had been caught by the system. Local police attribute this to the deterrent effect the system has on terrorists and criminals, but detractors simply claim this proves the system simply does not work.[61]

Florida, again in 2001, deployed another system in Ybor City, a popular tourist location. Video cameras snapped pictures of faces for comparison against a database of 30,000 that included runaway teens and people wanted on criminal charges.[62] In one case, the police used the image of a man, eating lunch in Ybor City, to demonstrate the system on local TV news. A

[57] Id. (The system installed was a product of Lau Technologies, Inc., a commercial vendor.)
[58] *At* http://www.findbiometrics, com/Pages/dace_articles/face_2.html (accessed November, 24, 2005).
[59] *At* http://www.wired.com/news/culture/0,1284,56878,00.html (accessed October 5, 2005).
[60] Electronic Privacy Information Center, *EPIC Face Recognition Information Page*. http://www.epic.org/privacy/facerecognition (accessed October 15, 2005). (The system installed was developed by Visionics, Inc., a commercial vendor.)
[61] *At* http://aclu.org//privacy/spying/14874prs20030902.html (accessed November 25, 2005).
[62] *Tampa puts face-recognition system on public street*, USA Today, July 13, 2001 at http://www.usatoday.com/tech/news/2001-07-13-tampa-surveillance.htm (accessed November 21, 2005).

woman in Oklahoma saw the picture and accused the man of being her deadbeat husband who owed her child support. The police approached the man who turned out never to have been married.[63]

The airport deployments attempted consist of cameras attempting to locate faces of pilots entered into a database to evaluate the systems in spotting potential terrorists. Accurate detection of even this limited database has been in the 30% - 50% range.[64] In all of these deployments, the common criticism is that innocent people come under suspicion and that true criminals go undetected.[65]

The privacy issues implicated by facial recognition technology are not so easily summed up, however. Hyper-surveillance technology in general, and automated facial recognition technology in particular, triggers both criminal procedure and constitutional privacy analysis on several levels. As always, these issues overlap in both analysis and application.

Legal Issues

While virtually every governmental action interferes with personal privacy to some degree, the question in each case is whether that interference violates a command of the United States Constitution.[66] The landmark Supreme Court decision on privacy and searches in the criminal context is *Katz v. United States*.[67] *Katz* provided a detailed analysis of what

[63] *See* Scott Berinato, *Face Recognition Hype is Over,* November 1, 2003, CIO Magazine *at* http://www.cio.com/archive/110103/tl_biometrics.html (accessed October 15, 2005) (New York, Chicago, and Washington D.C. have also instituted trial deployments.) State laws for civil privacy exist but no similar statutes exist in the federal system. In the case of mistaken identity, a common law action for false light and/or defamation may be possible.
[64] Id. Airports included in these studies include Boston Logan, Palm Beach International, Green International Airport, Dallas / Fort Worth, St. Petersburg-Clearwater, Fresno, LAX, and Oakland International.
[65] *At* http://aclu.org//privacy/spying/14874prs20030902.html (accessed November 25, 2005).
[66] *See* Warren & Brandeis, *The Right to Privacy*, 4 Harv. L.Rev. 193 (1890).
[67] 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576.

constituted a search under the Fourth Amendment of the United States Constitution.[68] More specifically, *Katz* defined an individual's privacy expectation in relation to the government's definition of a search.

One of the most enduring and significant concepts to be articulated in *Katz* is that the "Fourth Amendment protects people, not places."[69] This conceptual distinction may be of use when legislatures of the future consider protections against pervasive monitoring of the population, but for now it does not stand for a legal standard of much use in that regard. The reason for this is that "contemporary Fourth Amendment jurisprudence differentiates pervasive video surveillance from more familiar mass suspicionless searches in one crucial respect: by holding that it is not a 'search' at all."[70]

This is because while the first prong of the *Katz* test is subjective, the second prong is not.[71] In fact, *Katz*, which still provides the key legal test for what constitutes a search, provides that "what a person knowingly exposes to the public…is not a subject of Fourth Amendment protection."[72] Thus, even when the police scan a crowd with powerful binoculars in search of a particular person, they are not engaging in a Fourth Amendment "search." Video or still camera scans for persons are likewise non-protected searches under *U.S. v. Torres*, a

[68] U.S. CONST. amend. IV. "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."
[69] Katz v. United States, 389, U.S. 347, 351 (1923).
[70] Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 Miss. L.J. 213, 236 (2002) (listing fourteen cases that hold that public surveillance is not a search because any expectation of privacy would be unreasonable).
[71] The first prong accounts for the individual's expectation of privacy in a given situation. The second prong is the court's expectation. This second prong removes the danger that unrealistic individual expectations will result in privacy where society expects there to be none as well as the danger of government "training" the individual to have a skewed subjective expectation that serves law enforcement to society's overall detriment.
[72] Katz, 389 U.S. at 351.

1984 Seventh Circuit decision in the District Court of Appeals.[73] These decisions provide that suspicionless examinations are outside of the Fourth Amendments protections so long as they occur in public spaces and do not wander into private homes, offices, or other enclosed areas. Additionally, the adage that there is no "reasonable expectation of privacy" in conducting illegal activity still has merit.[74]

This approach was validated in *United States v. Knotts* in 1983.[75] In *Knotts*, law enforcement officials affixed a tracer into a container of chemicals purchased by the defendants. They then monitored the location of the container as it was transported to a cabin in the woods. The Court held that any information about the container that was available so long as it was in public view was fair game; the use of the tracer did not alter the nature of the surveillance.

Modern video networks pose a unique situation, however. Rather than a single instance of examination, these networks provide an opportunity for law enforcement to track a person's movements through public spaces. Such tracking would invariably result in much that an individual would rather not share with any audience much less have incorporated into official records. A person usually cannot enter a psychiatrist's office, marriage-counseling center, abortion or infertility clinic except from a public street. It is often in public that people ask others out on a date, join a religious community, or participate in a political demonstration. Of

[73] 751 F.2d 875. (Torres extends the Katz doctrine in public spaces to devices that merely "enhance" the sensory qualities of humans. The enhancement can be one of sensitivity or quantity. This is distinct from devices that provide "new" sensory powers, such as thermal imaging infrared detectors that can "see" through walls. The latter devices remain in a separate category and require warrants for use if their fruits are to be included as evidence in court. Additionally, such devices are not in general use by the public. Mainly, it is the type of information obtained by the use of these technologies that inform their admissibility; if searching the contents of a suitcase is permitted, then it matters not whether that search is conducted by opening the suitcase, x-raying the suitcase, or squeezing its sides. If the contents are protected, then any of these methods will not yield admissible evidence. *See generally* Kyello v. U.S., 533 U.S. 27 (2001))

[74] *See* Rakas v. Illinois, 439 U.S.128, 143 (1978). In Rakas, the Court noted that an individual conducting criminal activity may have a subjective expectation of privacy, "but it is not one which the law recognizes as legitimate." Id.

course, even in these deeply personal activities there is a chance we will be photographed or filmed by others nearby. But such third parties are unlikely to know who we are, where we came from and where we are going to go next.

In contrast, a government agency armed with a comprehensive visual record of our public activities would not have to guess when we would reveal personal information in public. It could in fact probe our lives after the fact and quickly build a more complete picture by tying in information contained elsewhere in its substantial database of recorded images and other sources of personal information now routinely on file. This sequence sets criminal procedures on finding probable cause in reverse: unwarranted activity searches can lead to probable cause rather than probable cause establishing reason to warrant a search.

In the context of searches on school grounds, the Supreme Court has recognized privacy and given force to Fourth Amendment protection when a principal looks through a student's purse, for example.[76] Students "may find it necessary to carry with them a variety of legitimate, non-contraband items and there is no reason to conclude that they have necessarily waived all rights to privacy in such items merely by bringing them onto school grounds."[77] Likewise, while commenting on a roadblock program on public highways, the Court emphasized that "people are not shorn of all Fourth Amendment protection when they step from their homes onto public sidewalks. Nor are they shorn of those interests when they step from the sidewalks into their automobiles.[78]

The point is that, while being surveilled by a comprehensive network of cameras and identity explicating software, one ceases to voluntarily expose information in the public sphere

[75] 460 U.S. 276 (1983).
[76] *See* New Jersey v. T.L.O., 469 U.S. 325, 333 (1985).

by merely traveling through it. While the Court has recognized things that are hidden in a car or a container, the same logic applies with equal force to the activities captured by public cameras: it is difficult, if not impossible, for individuals to avoid providing significant evidence of thoughts and personal interests as they walk on a public street via their facial expressions, interactions with others, and choices of activities. Such a string of information likely would be more revealing about a person than a single search through a purse, wallet, or even a file cabinet. Yet, contemporary jurisprudence provides Fourth Amendment protection to only the lesser of these two intrusions.

On a more basic level, the ability to simply identify an individual while they are in public, devoid of any tracking information, is a violation of the First and Fourth Amendments under some interpretations. A classic, and romantic, expectation of privacy is of one's identity when traveling within a crowd. Even in public, if one seeks to preserve their identity as private, it may be constitutionally protected according to *Katz*. While it is true that use of facial recognition technology does not force anyone to orally identify themselves, their identity is none-the-less revealed regardless of their wishes. Recent court decisions in this area, however, indicate that identity may no longer be a protected privacy interest. A recent Nevada decision that represents another expansion of the original Terry stop ruling makes silence regarding identity a criminal act.

The Terry doctrine describes the power of law enforcement to "stop and frisk" individuals as a narrow exception to the requirement that government seizures be the result of an

---

[77] Id. at 339. The Court ultimately decided that the principal did not need a warrant because, under the circumstances, such a search was reasonable. Id. at 340-41. However, the Court did not exempt the search of the purse from the scope of the Fourth Amendment. Id. at 336-37.

[78] Delaware v. Prouse, 440 U.S. 648, 663 (1979) (citation omitted).

articulated probable cause.[79] The need for officers investigating nascent crime to protect themselves is an obvious one. Though the Warren court was uncomfortable in allowing this expansion of police power, it permitted the expansion by balancing the need of law enforcement against the rights of society. The Terry procedure was seen as a seizure and an intrusion upon one's liberty interest, and the original doctrine was designed to be as unobtrusive as possible: only what was required to ensure safety was permitted.

Initially designed to allow officers to protect themselves, and those nearby, when confronting an individual, the Terry doctrine has been expanded dramatically over the years. The power now includes moving suspects and their passengers to different locations, detaining suspects for extended periods of time, handcuffing and pointing weapons at suspects, and forcing suspects to lie prone on the ground.[80]

This expansion has been caused partially by the creation of the "reasonable suspicion" standard, a standard established by facts observed by an officer and inferences derived from those facts that, considered as a whole, "reasonably warrant [the] intrusion."[81] Far less burdensome to law enforcement than a probable cause standard, reasonable suspicion is an unsettling development that erodes personal protections.

A 2004 decision, *Hiibel v. Sixth Judicial District Court of Nevada*, added additional powers to the Terry doctrine when the court ruled that officers could compel suspects to identify themselves when detained pursuant to a lawful Terry stop.[82] This new element of a police encounter implicates the First Amendment protection of speech, or more accurately, the right not to speak.

---

[79] *See* Terry v. State of Ohio, 392 U.S. 1 (1968).
[80] E. Martin Estrada, *Criminalizing Silence: Hiibel and the Continuing Expansion of the Terry Doctrine*, 49 St. Louis U. L.J. 279 (2005).
[81] Terry at 21.

Hiibel involved the constitutionality of a state "stop and identify" statute.[83] Such statutes typically permit police to question those suspected of recent or impending criminal activity and to obtain identification. Refusal constitutes grounds for further detention.[84] The practice had neither been prohibited nor upheld though it was subject to scrutiny as requiring "objective criteria of specific suspicion."[85] The constitutionality of such statutes was in doubt and lower courts were split on the issue. In *Hiibel*, the Court resolved the split in favor of the constitutionality of "stop and identify" statutes.

What is most troubling about this decision in a world of networked cameras capable of identifying anyone without their permission is that it lays the groundwork for an exception to what had been strong First Amendment protections against compelled speech. If compelled speech is permissible in a police context, then how can one argue that having one's identification wrested from them is protected?

Precedent has established that students must not be compelled to recite the Pledge of Allegiance nor drivers be compelled to include state mottoes on their vehicle registration tags.[86] The prohibition on compelled speech specifically covers factual information as well. In *Talley v. California*, the Court held unconstitutional an ordinance requiring a publicly distributed handbill to contain the name and address of its sponsor.[87] The Court expressed its high regard for anonymity recalling the important role played by anonymous speech in the Revolutionary War, stating: "[i]t is plain that anonymity has sometimes been assumed for the most

---

[82] *See* Hiibel v. Sixth Judicial District Court of Nevada, 124 S. Ct. 2451 (2005).
[83] Id. at 2456.
[84] Uniform Arrest Act of 1942 § 2 28 Va. L. Rev. 315,320-321 (1942).
[85] *See* note 74 supra at 290.
[86] *See* West Virginia State Board of Education v. Barnette, 319 U.S. 624 (1943) and Wooley v. Maynard, 487 U.S. 781 (1988).
[87] 36 U.S. 60 (1965).

constructive purposes."[88] Years later, in *McIntyre v. Ohio Elections Commission*, the Court again noted that "[a]nonymity is a shield from the tyranny of the majority."[89]

In 1999, a federal district court in the Seventh Circuit decided a case that underscores the value of one's anonymity in the political and religious context. In *American Knights of the Ku Klux Klan v. City of Goshen*, the city Goshen, Indiana had passed an ordinance prohibiting the wearing of masks for the purpose of concealing identity in public.[90] This case could easily foreshadow a future ordinance enacted for the purpose of foiling attempts to defeat a future facial recognition system. In the instant case, the purpose was to deter Klan activities, and the Klan challenged its constitutionality.

The court held that the ordinance, by prohibiting plaintiff's members the right to wear masks for the purpose of concealing identity in public, burdened the free speech and association rights of plaintiff's members. Even though the record reflected that some Klan members appeared in public without masks, the court found that "[o]ne person's choice to reveal his or her identity does not delimit another person's First Amendment rights."[91] The choice to reveal your identity is a personal one and Constitutional rights attach individually.

Hiibel represents a shift away from the recognition that the right not to speak is on par with the right to free speech and that anonymity and autonomy are valuable rights related to one's public image. Furthermore, since the *Hiibel* decision was made in the context of a Terry stop scenario, it implicates Fourth Amendment protections as well.

Originally, an individual was not penalized for silence during a Terry stop: while officers may ask questions of the detainee, "the person stopped is not obliged to answer, answers may

[88] Id. at 65.
[89] 514 U.S. 334, 357 (1995).
[90] *See* American Knights of the Ku Klux Klan v. City of Goshen, 50 F.Supp.2d 835 (1999).
[91] American Knights of the Ku Klux Klan at 839.

not be compelled, and refusal to answer furnishes no basis for an arrest, although it may alert the officer to the need for continued observation."[92] The *Hiibel* Court apparently sees Justice White's comments as dicta and uses that classification to reason around the plain meaning of the text. Clearly, however, one's identity is worthy of protection, particularly in a society where, for example, an identity is often the object of theft. Furthermore, supplying an identity to the government is completely different from consensual disclosure to third parties for purposes of commerce.

The government has the capacity to link an identity to a storehouse of personal data. It is this "data fusion" that gives great power to a mere identity in modern times. The difference between being compelled to open the trunk of your car and to divulge your identity is a matter of method; both acts amount to the revelation of a significant quantity of personal information. Additionally, the Court has indicated that while the use of technology to enhance investigatory capabilities does not automatically establish a search, it is more likely that a search has occurred within the meaning of Katz when that technology "is not in general public use" and circumvents the protections of the Fourth Amendment.[93] State-of-the-art facial recognition networks certainly fit the *Kyello* parameters.

The context for the introduction of facial recognition software is of course the new threat posed by terrorism. The *Hiibel* court stated that "[m]ost importantly, we are at war against enemies who operate with concealed identities and the dangers we face as a nation are unparalleled."[94] While the dangers are great, they are not new. Many times in our past national emergency has required that we confront dangers both abroad and domestic and in doing so evaluate our responses against the fundamental principals that define our social and political

[92] Terry v. Ohio, 392 U.S. 1, 34 (1968) (White, J., concurring).
[93] Kyello v. U.S., 533 U.S. 27, 40 (2001).*See also* note 70 supra.

existence. Certainly, prevention of domestic terrorist attack is a legitimate government interest. That interest needs to be balanced against the level of intrusion a mass, suspicionless and random search imposes upon the citizenry.

Political and Philosophical Considerations

It is imperative to recognize that we endeavor to live in a free society. An essential component of a free society is some level of privacy. If the goal of law enforcement vis-a-vis terrorism is to protect this free society, then we must ensure that the means do not sacrifice that end. Perhaps in this new age it is important to define exactly what constitutes privacy.

Privacy is that feature of our existence that dictates that others do not have access to our data at their discretion. Sometimes, this will mean that we can control who has access to ourselves and other times it will mean a total denial of access. The value of privacy lies in our being able to make this distinction at will; the power to allow or deny others of their access to ourselves.

When the need for that power exists, there is a moral case for privacy. When that power is given legal effect, a right of privacy is established. Such rights are in tension with the needs of a functioning society so that certain tradeoffs must be made for the good of the collective. Therefore, we must value our privacy accordingly so that effective decisions may be made that safeguard our physical coexistence while preserving our private existence.

Facial recognition system networks, when fully operational and deployed, will have affects that we must now project in order to fully understand potential penalties. Let us imagine such a network is in place. How might it affect our daily existence?

---

[94] Hiibel v. Sixth Jud. Dist. Ct. ex rel. Humbolt, 59 P.3d 1201, 1206 (Nev. 2002).

First is the effect upon on our behavior that might occur from the knowledge of our being observed. This is a loss of extrinsic freedom, in which a lack of privacy makes us vulnerable to having our behavior controlled by others. Those who engage in unpopular or unconventional activity will face pressures in the form of the denial of certain benefits, jobs, and promotions. This is likely to have a chilling effect that constrains the range of freedom to act. "Privacy functions to promote liberty of action, removing the unpleasant consequences of certain actions and thus increasing the liberty to perform them."[95]

In a free society, many actions thought immoral by a majority are not deemed illegal. Each individual is free to decide for themselves what actions to take. Such subjects include pornography, gambling, drunkenness, homosexual or extra-marital sex. If it would be wrong to force people legally to conform to the majority's views on such issues, it will be equally wrong to use harsh social pressures to accomplish the same effect. It is for this reason that Mill argued, in *On Liberty*, against both legal enforcement of morality and its informal social enforcement by stigmatization or ostracism.[96] "Threatening the minority with stigmatization or ostracism works like force because it changes people's actions by attaching painful consequences to them without changing their minds at all."[97]

Secondly, a facial recognition network would cause a loss of intrinsic freedom. This refers to a loss of choice not due to outside pressures, but due to a lack of privacy the choice itself no longer exists for us to make. Who has access to our personal history, for example, will be a choice taken from our control. Another aspect of this loss is how the performance of an act is affected by its being performed within view of another. Every act performed becomes

[95] RICHARD WASSERSTROM, PRIVACY: SOME ARGUMENTS AND ASSUMPTIONS IN PHILOSOPHICAL DIMENSIONS OF PRIVACY 325-26 (Ferdinand Schoeman, ed., 1984).
[96] JOHN STUART MILL, ON LIBERTY 9 (Hackett Publishing Company, 1978; originally published in 1859).

the act itself and the record of that act. This is analogous to having a conversation with someone in your imagination versus leaving a message on his or her answering machine. In a society of recorded actions, one is no longer free to simply act without the record. This is a loss of the freedom to act spontaneously because every act, no matter how innocent, would become a part of the record.

Third, our inability to withdraw from observation tells us that we lack authority within our society. Individualization, privacy, is absent already from organizations such are armies, churches, monasteries, communist cells, and other groups where common goals outweigh individual needs and desires. We join these groups of our own accord, for our own reasons. This gives value to not being a member of such groups. Therefore, when our retained privacy is breached, it is an insult to our person, an assault on our autonomy and authority to remain autonomous. "The symbolic message of constant government observation is loss of ownership to ourselves by announcing that our every move is fitting data for observation by others. As a symbolic message, it insults rather than injures."[98]

Fourth, a lack of privacy is the logical result of a culture that simplifies life in every other respect for its supposedly adult members. When Socrates said "[A]n unexamined life is not worth living," he surely meant self examination. A society that examines your life for you further destroys the desire and the need for the individual to do the heavy lifting. "Such an individual merges with the mass. Such a being, although sentient, is fungible."[99]

It is axiomatic in our society that greater privacy is afforded to adults than to children. Is it so unthinkable to imagine that as privacy is withdrawn from adults, more childlike behaviors

---

[97] Jeffery H. Reiman, *Driving to the Panopticon: A Philisophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future* 11 Santa Clara Computer & High Tech. L. J. 27 at 36.
[98] Id. at 39.
[99] Id. at 41.

will surely follow? Like a child, as the outer expression of ourselves grows in importance, the inner core of our selves will be diminished, the inner personal core that "is the source of criticism of convention, of creativity, rebellion and renewal. The art of such people will be insipid decoration and their politics fascist."[100]

Liberalism in our society has often been protected by the law through use of the "slippery slope" argument. In the case of government deployed, automated and intelligent surveillance systems, and the events that will lead up to it, the threat has rather been more like the death of liberalism by a thousand cuts.

> The liberal vision is guided by the ideal of the autonomous individual, the one who acts on principals which she has accepted after critical review rather than simply absorbing them unquestioned from outside. Moreover, the liberal stresses the importance of people making sense of their own lives, and of having authority over the sense of those lives. This requires a kind of space in which to reflect on and entertain beliefs, and to experiment with them – a private space.[101]

Our constitutional safeguards are material conditions for privacy more real and reliable than mere formal conditions accepted as part of societal convention. We require strong material protections because technologies like cameras and data fusion are material tools for the invasion of privacy. When we are told we must give up some of our freedom for the sake of security, we must not accept that statement at face value. We must recall that while these conditions are new in application they are not new in affect and as Benjamin Franklin wisely said at the outset that the man who does sacrifice his liberty for security receives neither.

The Potential for Extralegal Abuse and Legal Remedies

Courts require time, an established controversy, and a factual history to establish standing and to reach solid decisions. Realistically, it is hard to see, given the *Katz* doctrine and the

[100] Id. at 42.
[101] Id.

result of *Knotts*, why courts would suddenly find camera surveillance a search under the meaning of the Fourth Amendment. Meanwhile, the potential for abuse of the information gathered is high. In the past, government abuse of investigatory powers has occurred with the aim of chilling political or religious speech and punished some forms of association. How can society use the lessons of the past to deter such abuses from occurring in the future? If legislation is the answer, then how can we design such legislation for maximum effect?

The history of the FBI and other law enforcement surveillance provides little comfort to those engaged in lawful political and religious activities that are concerned about becoming a target of surveillance. From its inception until restrictions on its activities were imposed in the mid-1970s – and even sometimes thereafter – the FBI regularly conducted politically motivated surveillance, choosing targets based on their political or religious beliefs.[102] During the Vietnam war, the CIA, despite restriction of its mission to foreign intelligence, also conducted domestic surveillance operations.[103] Religious groups engaged in political activity were among the targets of intelligence agency investigations.[104]

With today's focus on anti-terror tactics, it is no wonder that Muslims who frequent mosques and Islamic centers, particularly those that express religious or political views considered "extreme," are now concerned about being subjected to abusive and unjustified law enforcement behaviors similar to those documented by the Senate Committee to Study Governmental Operations with respect to Intelligence Activities in 1976.[105] Without external

[102] Declan McCullah, *Call it Super Bowl Face Scan I*, Wired News, at http://www.wired.com/news/politics/0,1283,41571,00.html (accessed October 21, 2005).
[103] Quentin Burrows, *Scowl Because You're on Candid Camera; Privacy and Video Surveillance*, 31 Val. U. L. Rev. 1079 (1997).
[104] Id.
[105] Linda E. Fisher, *Guilt by Expressive Association: Political Profiling, Surveillance and The Privacy of Groups*, 46 Ariz. L. Rev. 621 at 623.

constraints, law enforcement almost invariably investigates dissidents based on their political or religious expression.

The FBI has recently admitted to surveilling mosques in nine U.S. cities and to keeping certain Muslims in the U.S. under intensive surveillance.[106] In 2003, the New York City police department questioned arrestees at antiwar demonstrations about their political affiliations and entered that information into a database.[107] These are but a few of the reports of recent political or religious infringement that has become known since September 11, 2001.

> The Supreme Court's expansive construction of the First Amendment-based right of association, as originally defined in NAACP v. Alabama and delineated most recently in Boy Scouts v. Dale, can protect groups engaged in First Amendment conduct from unjust political or religious surveillance that causes them cognizable harm. Because privacy in association is fundamental to the First Amendment, because surveillance carries a significant harm to expressive association, and because a group's conception of the conduct that would interfere with its expression must be taken into account, the right of association may outweigh the State's interest in appropriate instances.[108]

Political association enhances democracy and is considered a civic virtue. It is a cornerstone of a free society. Yet, a network of facial recognition enabled cameras tracking the movements of individuals merely associated with a perceived dangerous individual or institution would certainly chill expression among those actually guilty of nothing at all beyond that association. Further, identification of individuals associated with a group could induce members to withdraw and dissuade others from joining because of fear of exposure of their beliefs and the consequences of this exposure.[109]

Legislation is needed to prevent political surveillance absent at least a reasonable suspicion that criminal activity is taking place. "Politically motivated investigations are not

---

[106] *See* U.S. House of Representatives, Committee on the Judiciary, Sensenbrenner/Conyers, Release Justice Department Oversight Answers Regarding USA PATRIOT Act and War on Terrorism, May 20, 2003, at 39-40. Available at http://www.house.gov/judiciary/patriotlet051303.pdf, (informal survey of FBI field offices revealed that fewer than ten have investigated mosques since September 11).

[107] Joyce Purnick, *Speak Out. The Police Are All Ears*, N.Y. Times, April 21, 2003, at B1. Police ceased this practice once it came to light. Id.

permissible since the mission of law enforcement is to enforce the criminal laws, not to monitor political or religious expression."[110]

Facial recognition technology can be, if abused, a hyper-intrusive technology. It will permit a computer to scan images of a crowd or demonstration and match the individuals there almost instantly to a database of information on known individuals. It is over broad (in that it retrieves far more information than it seeks), indiscriminate, occurs without notice, is ongoing, and poses an unusual threat to human dignity. Legislators have recognized these factors in other contexts and have created statutory rules and restrictions to control the use of such searches.[111]

In 1968, Congress passed a series of legislation regarding hyper-intrusive searches known as Title III to the Omnibus Crime Control and Safe Streets Wiretap Act. Title III covers interception of all oral and wire communications. To conduct such a search, law enforcement must seek and receive a "Title III order" from a federal judge. The requirements for such an order are much greater than what is required for a standard search warrant.

Law enforcement must show that normal investigative procedures have been tried and failed, are likely to fail, or are dangerous.[112] The surveillance must be carried out in a way that minimizes the interception of irrelevant information.[113] There must be probable cause to believe an interception will reveal evidence of one of a list of specific predicate crimes.[114] The order must be authorized by a high-level Justice Department official and signed by a federal

---

[108] Note 99 infra at 624. NAACP v. Alabama, 357 U.S. 449 (1958). Boy Scouts v. Dale, 530 U.S. 640 (2000).
[109] NAACP , 357 U.S. at 463.
[110] Note 99 infra at 627.
[111] *See* Federal Communications Act of 1934, 47 U.S.C. § 605 (2004) (prohibiting wiretapping of telephones after the Supreme Court had declared the practice constitutional in Olmstead v. United States, 277 U.S. 438, 466 (1928)).
[112] 18 U.S.C. § 2518 (3) (c) (2000).
[113] 18 U.S.C. § 2518 (5) (2000).
[114] 18 U.S.C. § 2518 (4) (c) (2000).

judge.[115] The order is time limited to thirty days, though a government official can request an extension.[116]

In recent years Title III has been extended to e-mail and other forms of electronic communication but, inexplicably, not to video surveillance. It is ironic indeed that facial recognition tied to a network of cameras is not yet considered hyper-intrusive under current Fourth Amendment jurisprudence because of the element of public places alone. Surely the high volume and quality of information made available by tracking someone's movements through the public domain alter the activity into a cognizable search.

But even statutory protections, such as Title III and Electronic Communications Privacy Act (ECPA) are not reliable protections in a shifting political climate. Enactment of the PATRIOT Act shows that statutory protections are relatively easy to alter. And the Courts have reconciled this with *Katz* and its progeny: we have no reasonable expectation of privacy in the identity of people we telephone, e-mail, nor in the identity of the people who e-mail us back. Once we acknowledge that telephone pen registers/traps are not searches, as was done in *Smith v. Maryland*, the challenges of the ECPA and Title III are little more than logical adaptations of the doctrine for new media or camera surveillance.[117]

In addition, law enforcement regularly seeks to roll back legislative protections in the name of national need or emergency. Recently, for example, the Defense Intelligence Agency sought to "loosen decades-old restrictions, asking Congress to allow its intelligence agents to go undercover when they approach Americans who may have useful national-security

[115] 18 U.S.C. § 2516 (2000).
[116] 18 U.S.C. § 2518 (5) (2000).
[117] 442 U.S. 735 (1979) (holding that once a person enters calling information into the telephone company's system, they have assumed the risk that the telephone company will divulge that information to authorities. Combined with the Katz doctrine, this may be used to justify many intrusions into where there may be a subjective expectation of privacy).

information, rather than identifying themselves as intelligence operatives."[118] Even as the government seeks to conceal the identity of its operatives, it seeks to strip the citizenry of its right to maintain their own identity as private.

Conclusion

Facial recognition technology combined with video surveillance is a technology with much promise for increased security and efficiency but which requires potent and far reaching oversight to prevent an erosion of liberties and freedoms and to prevent outright abuse. Effective oversight can ameliorate the effects of privacy reductions, the chilling effects on human behavior, the growth of the "police state," and the discriminatory targeting of certain groups. Damage to property interests in personal identity and photographic images can be limited by careful control and security of databases and ensuring the reliability of the technology prior to deployment. A well earned belief in the authority's responsible use of the technology can limit the interference with freedoms to speech and association.

The actual use of facial recognition technology in practice remains an open question. Will it be used like an Automatic Fingerprint Identification System, where a machine makes an initial match, and a human operator makes the final determination? If so, then the issues inherent with eyewitness identification may come into play. In that scenario, courts have found that no expert is needed as juries are capable of comparing faces and determining whether there is a valid match or not.[119] If the machine is to make the final determination, then expert testimony regarding the operating efficiencies and accuracy's of the system will be needed. Will juries be overwhelmed by the technology and simply rubber-stamp a match as valid? Another question is how law enforcement will handle false positives. Such events will have an

[118] Katherine Shrader, *The Pentagon Wants to Talk to You – On the Sly*, Associated Press, October 18, 2005.

adverse effect on the liberty interest of any individual identified by the system in both investigative and probative scenarios. What recourse will an individual have if falsely accused and detained?

Currently, there is no case or statutory law that adequately deals with new biometric technologies. A general right to privacy may need to be recognized before new technologies can be implemented in society and still preserve the qualities of a liberal democracy. Courts likewise have a number of possible responses to intrusive searches. Courts can ban the searches altogether or force government agents to meet stricter requirements to initiate and conduct such a search. This was the route chosen by Congress in creating Title III, for example. It is for vigilance and critical examination of the new uses of technology that are the most important and general safeguards for which we can strive. That means that courts and legislatures must draw from the expression and expertise of all our varied disciplines in order to provide the context and empathy needed to balance the needs of a secure society against the human spirit we wish to nourish and protect.

[119] United States v. Smith, 122 F.3d 1355, 1359 (11th Cir. 1997).