Innovations in Election Administration 18

Using Biometric Identification Technologies in the Election Process

Using Biometric Identification Technologies in the Election Process

Author:
Dr. Jim Wayman
Director
U.S. National Biometric Center
College of Engineering
San Jose State University

Managed and Edited by:
William C. Kimberling
Office of Election Administration
Federal Election Commission

Published by:
Office of Election Administration
Federal Election Commission
Washington, D.C. 20463

September 2001

Introduction by the Office of Election Administration

This report is another in the series on Innovations in Election Administration being published by the FEC's Offfice of Election Administration.

The purpose of this series is to acquaint State and local election officials with innovative election procedures and technologies.

Our reports on these innovations do not necessarily constitute an endorsement by the Federal Election Commission either of any specific procedures described or of any vendors or suppliers that might be identified within the report. Moreover, the views and opinions expressed in these reports are those of the authors and are not necessarily shared by the Federal Election Commission or any division thereof.

We welcome your comments on these reports as well as any suggestions you may have for additional topics. You may mail these to:

Office of Election Administration
Federal Election Commission
999 E. Street, N.W.
Washington, D.C. 20463

or else contact us

Toll free on 800.424.9530 (option#4)
Direct on 202.694.1095

or else by e-mail at

bkimberling@fec.gov.

Using Biometric Identification Technologies in the Election Process

Biometric technologies, allowing the automatic identification of people using voice patterns, eye scans, handwriting style, faces, hands or fingerprints, have been suggested for use in the election process for eliminating fraud. Fingerprinting, hand shape, and eye scanning have been used in the United States in driver licensing and social service programs. Fingerprinting systems are being introduced into the election process in several countries, such as the Philippines, Jamaica, Argentina, and Cambodia. What are the prospects for introducing these technologies into our voting systems?

We will look at the possible voting applications in this paper and conclude that biometric technologies could be effectively used, even on a voluntary basis, to detect and deter voting fraud. However, this use would require fundamental changes in the way we register voters and would necessitate the creation of government-controlled databases of physical and behavioral characteristics of at least some voters. Although such databases are inherently "fuzzy" and far less threatening to personal privacy than phone books or driver's licenses, changes in voter registration procedures to enable biometric data collection could be seen as contrary to the intent of the National Voters Rights Act of 1993 and would likely require enabling federal legislation.

What is Biometric Identification?

Biometric technologies use physical characteristics, such as voice tone or hand shape, to identify people automatically. Behaviors, such as handwriting style, can also be used by computers in this way. The term "identify" is used here quite loosely. There is actually nothing in your voice, hand shape or any biometric measure to tell the computer your name, age or citizenship, or to establish your eligibility to vote. External documents (passport, birth certificate, naturalization papers) or your good word establishing these facts must be supplied at the time you initially present yourself to the biometric system for "enrollment". At this initial session, your biometric characteristic, such as an eye scan, is recorded and linked to this externally-supplied personal information. At future sessions, the computer links you to the previously supplied information using the same physical characteristic. Even if the biometric system works perfectly, the personal data in the computer, such as your voting eligibility, is only as reliable as the original "source" documentation supplied.

Once the computer knows your claimed identity, it can usually recognize you whenever you present the required biometric characteristic. No biometric identification system, how-

ever, works perfectly. Problems are generally caused by changes in the physical characteristic. Even fingerprints change as cuts, cracks and dryness in the skin come and go. It is far more likely that the computer will not recognize your enrollment characteristic than link you to the characteristic of someone else, but both types of errors do occur.

Id ntification: Positive and Negative

Biometric systems are of two types: "verification" and "identification". We prefer the to use the descriptions *"positive identification"* and *"negative identification"* to emphasize the opposite nature of two approaches.

A positive identification system requires you to identify yourself when submitting a biometric measure. Your submitted measure is then checked against the measure given when you enrolled in the system to affirm that they match. Biometric measures are always "fuzzy" to some extent, changing over time and circumstance of collection. If the submitted and stored biometric measures are "close enough", it is assumed that you are indeed the person enrolled under the identity you claimed. If the presented and enrolled characteristics are not "close enough", you will generally be allowed to try again. If multiple attempts are allowed, the number of users "falsely rejected" can be under 1%, although there are always some people chronically unable to use any system who must be given alternate means of identification. The possibility that an impostor will be judged "close enough", even given multiple attempts, is usually less than one in ten. The threat of being caught in 9 out of 10 attempts is enough to deter most impostors, particularly if penalties for fraud are involved.

Positive identification using biometrics can be made totally voluntary. People not wishing to use the system can instead supply the source documents to human examiners each time they access the system.

TABLE 1: IDENTIFICATION: "POSITIVE" AND "NEGATIVE"

POSITIVE	NEGATIVE
To prove I am someone known to the system	To prove I am not someone known to the system
Comparison of submitted sample to single claimed template	Comparison of submitted sample to all enrolled templates
Alternative identification methods exist	No alternative methods exist
Can be voluntary	Must be mandatory for all
Biometric measures linked to personal information (name, age, citizenship) only through external source documents.	Linkage to personal information not required.

In "negative identification" applications, found in driver licensing and social service eligibility systems where multiple enrollments are illegal, a user claims not to be previously enrolled. In fact, a negative identification biometric system does not require any identity claim by the users. If a user offers an identity, it is only for the purpose of linking to outside records to establish proof of age or citizenship. The biometric measures themselves cannot establish name, age, or citizenship and therefore do not prevent their misrepresentation during enrollment. These systems do, however, prevent a person from enrolling more than once under any identity. Apart from the "honor" system, where each person's word is accepted, there are no alternatives to biometrics for negative identification.

During enrollment, the system must compare the presented characteristic to all characteristics in the database to verify that no match exists. Because of the ongoing changes in everyone's body, errors can occur in the direction of failing to recognize an existing enrollment, perhaps at a rate of a few percent. But again, only the most determined fraudster, unconcerned about penalties, would take on a system weighted against him/her with these odds. False matches of a submitted biometric measure to one connected to another person in the database are extremely rare and can always be resolved by the people operating the system.

Negative identification applications cannot be made voluntary. Each person wishing to establish an identity in the system must present the required biometric measure. If this were not so, fraudsters could establish multiple enrollments simply by declining to use the biometric system. On the other hand, negative identification can be accomplished perfectly well without linkage to any external information, such as name or age. This information is not directly necessary to prove you

are not already known to the system, although it may be helpful if identification errors occur.

What are the Technologies?

Many biometric methods have been used in public systems for "positive identification": hand and finger geometry, iris and retinal scanning, voice and face recognition, signature and fingerprinting.

Voice systems have the longest history, dating back to the 1950's. The National Institute of Standards and Technology (NIST) runs an annual competition for voice recognition technologies using speech sample collected over the telephone. Error rates (both not recognizing a person and falsely recognizing a person as someone else) are a few percent. Error rates increase if users do not consistently use the same telephone. Data storage is a few kilobytes of information for each user. Voice recognition is currently being used by the Immigration and Naturalization Service at some border crossings. These systems require no special hardware other than a microphone and a computer, so can be quite inexpensive.

Fingerprinting systems have been in use for almost three decades. Users are required to place a single finger on a glass "platen" to be electronically "imaged" (photographed) from underneath. Error rates vary considerably between vendors and a small percentage of people are unable to use these systems at all because of unsuitable fingerprints. The strong advantage of this method, however, is that people have multiple fingers, each with a different fingerprint. By requiring the use of multiple fingerprints, error rates can be made quite low for those able to use the system. Data storage is several hundred to a thousand bytes per user. Fingerprint scanners which link to a computer are now available for under $100 and computer keyboards with built-in scanners are also available. Access control systems using fingerprinting can be seen in prison and military applications.

Hand geometry systems have been in use for twenty-five years and have seen the largest number of fielded applications. The users place their right hand on a reflective surface and an electronic image is captured of its shape. No details, such as fingerprints, are seen; only the shape (similar to a shadow) of the non-reflecting hand. Error rates for regular users can be considerably under one percent, although error rates for infrequent users are higher due to their unfamiliarity with proper hand placement. A small percentage of people (perhaps 1%) cannot use these systems effectively due to hand irregularities. Data storage is only nine bytes per user. Standalone units are available for considerably under $1000. The Immigration and Naturalization System uses hand geometry systems in airports and at border crossings.

Finger geometry is a new method that has seen extensive use over the last three years at Walt Disney World, where over 10 million season pass holders have been verified. Users place fore and middle fingers (like a "peace" sign) into the device, where the general finger shapes (but not fingerprint details) are captured. Error rates for this device are unknown, but its successful use by Walt Disney World seems to indicate that a wide range of people can use it effectively. Data storage is 14 bytes per user. The device is available only as "OEM" hardware, thus requiring significant system integration.

Iris scanning is a new technology with the advantage that no direct contact between the user and the hardware is required. A black-and-white image of the user's eye is recorded from a distance. Successful use of this tech-

nology requires trained operators, cooperative users and well-adjusted equipment. Experimentally measured error rates for this technology are not known, but increase in the presence of uncontrolled lighting conditions. A few percent of people seem not to be able to use this technology. Data storage is about two kilobytes per user. Units with a supporting computer can be purchased for under $10,000. Several pilot projects using this technology are currently underway.

Face recognition is another emerging technology also studied by NIST. For this technology as well, no direct contact is required between the user and the hardware. Error rates have been measured at several percent and increase with time after enrollment to several tens of percent. Lighting conditions must be controlled for successful usage. Some percentage of people are unable or unwilling (such as veiled women) to use this technology. Depending upon the vendor, data storage can be as low as 256 bytes per user. Software packages for under $100 are available for computers with digital cameras.

Retinal scanning systems have been in use for fifteen years. Users are required to place their foreheads against a head rest and look at a small light. Error rates, as measured in a 1990 test funded by the Federal Highway Administration, showed no incorrect matches of different users, but 10% or higher failures to match. The percentage of people unable to use this equipment is unknown. Data storage is 72 bytes per user. A few retinal scanners are used inside the Pentagon to control access to classified spaces.

Automatic signature recognition is of two types: static and dynamic. Static signature systems attempt to recognize a written signature that has been optically scanned into a computer. Dynamic signature systems recognize hand movements during the signature process, not the signature itself, and require specialized hardware consisting of either a pen with embedded pressure sensor and accelerometers or a digital computer pad. Error rates for dynamic signature verification were measured in 1992 by a national laboratory. The rate of not recognizing known users was 2% when multiple attempts were allowed. Impostors were accepted at a rate of about 1% under these conditions. The percentage of persons unable to use this equipment is unknown. Data storage requirements range from 50 bytes to 2 kbytes per user. Units usable with personal computers can be purchased for a few hundred dollars or less.

Although we have wide experience with biometric devices in positive identification applications, only two types of biometric methods have ever been used in documented negative identification applications. Those methods are fingerprinting and retinal scanning. Pilot projects for use of iris scanning for negative identification are being planned and/or implemented.

TABLE 2: TECHNOLOGIES DEMONSTRATED IN DOCUMENTED PUBLIC SYSTEMS

POSITIVE IDENTIFICATION	NEGATIVE IDENTIFICATION
Hand geometry	Fingerprinting
Finger geometry	Retinal scanning
Voice recognition	
Iris scanning	
Retinal scanning	
Facial imaging	
Fingerprinting	

Will Biometric Identification Compromise Privacy?

Whenever biometric identification is discussed, people always want to know about the implications for personal privacy. If I use a biometric system, will the government, or some other group, be able to get personal information about me? Biometric measures themselves contain no personal information. My hand shape, fingerprints or eye scans do not reveal my name, age, race, gender, health or immigration status. Although voice patterns can give a good estimation of gender, no other biometric identification technology currently used reveals anything about me as a person. More common identification methods, such as a driver's license, reveal my name, address, age, gender, vision impairment, height and even weight! Unlike driver's licenses, however, biometric measures cannot be stolen or counterfeited.

The real fear is that my biometric measures will link me to my personal data, or allow my movements to be tracked. After all, credit card and phone records can be used in court to establish a person's activities and movements. There are several important points to be made on this issue.

Only biometric measurements which I have surrendered to a system through "enrollment" will be known to that system. If I have never enrolled (given my fingerprint with supporting identification documentation) in a fingerprint system any use I make of a fingerprint system cannot be linked to 'me' (my identity).

Biometric measures cannot generally be taken without my knowledge, so I cannot be enrolled in any system without my participation. Exceptions are face and voice patterns, which can be taken without my knowledge. "Latent" fingerprints left on surfaces can be "lifted" by those trained in investigative techniques, but such prints are generally not of a quality suitable for enrollment purposes in electronic systems.

Phone books are public databases linking me to my phone number. These databases are even accessible on the Internet. "Reverse" phone books also exist allowing my name to be determined from my phone number. Even

if I have an unlisted number, my number and all information on calls made from that number may be available to law enforcement agencies through the subpoena process. There are no public databases, however, containing biometric identifiers, and there are only a few limited-access government databases containing biometric measures. Eight States have electronic fingerprint records of social service recipients (AZ, CA, CT, IL, MA, NJ, NY, TX), five States (CA, CO, GA, HI, TX) maintain electronic fingerprints of all licensed drivers[1], nearly all States maintain copies of driver's license and social service recipient photos, the FBI and State governments maintain fingerprint databases on convicted felons and sex offenders, and the federal government maintains hand geometry records on those who have voluntarily requested border crossing cards. General access to this data is limited to the agencies that collected it, but like credit card and phone "toll records", this information can be released or searched by law enforcement groups acting under court order.

Unlike your legal name and your Social Security, credit card and phone numbers, your biometric measures are rather fuzzy and inexact, being somewhat different every time they are measured. Further, your biometric measures will be rather similar to the biometric measures of others. Consequently, even if you could gain access to a database containing biometric measures, they could not be "reversed" like a phone book to reveal names from identifying numbers. Two technologies, electronic fingerprinting and retinal scanning, have been objectively demonstrated to be exceptions to this reversibility rule, if data is carefully collected from cooperating users. So if you want to discover someone's identity, the best way is with a phone number, not a biometric identifier. If you want personal information about someone, start with their name; a biometric identifier will be of no help.

Biometric identifiers in databases of drivers, social service recipients or border crossers, are far less distinctive than the names, addresses and ID numbers also in these databases, and do not allow users to be tracked or monitored like credit card and phone numbers do. For this reason, databases of drivers and social service recipients are always indexed by name or identification number even if they contain a biometric record. Biometric identifiers are nearly impossible to steal or falsify than these other identifiers, allowing protection from identity theft or impersonation. In conclusion, adding a biometric identifier to current voter registration databases would not present any privacy risk to any voter, but could be used to *prevent or deter privacy loss* through identity theft.

[1] WV maintains a voluntary fingerprint database on drivers who wish to use biometric identification.

TABLE 3: BIOMETRICS AND PRIVACY

1) Unlike more common forms of identification, my biometric measures contain no personal information about me and cannot be stolen or forged.
2) Some biometric measures (face images, voice signals, and "latent" fingerprints left on surfaces) can be taken without my knowledge, but can't be linked to me without a pre-existing database.
3) The federal government maintains a fingerprint database on convicted felons and some State governments maintain fingerprint and image databases on drivers and social service recipients.
4) My social security or credit card number, and sometimes even my legal name, can identify me out of the entire U.S. population. This capability has not been demonstrated using any single biometric measure.
5) Like phone and credit card information, biometric databases can be searched outside of their intended purpose by court order.
6) Unlike your credit card, phone or Social Security numbers, biometric characteristics change from one measurement to the next.
7) Searching for personal data based on biometric measures is not as reliable or efficient as using identifiers like your legal name or your Social Security number.

Election System Goals

Biometrics have been successfully used to increase the integrity of the driver's licensing and social service benefit distribution processes in many States. There is no question that it is ***technically*** possible to use biometrics to limit fraud in voting processes as well. The 14th, 15th, 19th , 24th, and 26th Amendments to the U.S. Constitution establish voting as the right of all citizens 18 years of age or older who have not been convicted of a disqualifying crime. The recognition of voting as a "right", however, separates it from the identified "privileges" of driving and receiving social service benefits

Further, by federal law we have adopted the potentially competing goals of limiting fraud and enhancing voter registration. The National Voter Registration Act (NVRA) of 1993 seeks: (1) "...to increase the number of eligible citizens who register to vote in elections for Federal office....; (2) (to enhance) the participation of eligible citizens as voters in elections for Federal office; (3) to protect the integrity of the electoral process; and (4) to ensure that accurate and current voter registration rolls are maintained."

It is fair to say that these are the goals of the current Congress as well and should be our goals when suggesting changes to the voting process. Protecting the integrity of the electoral process should include making sure that only eligible voters register, and that only registered voters cast vote. It seems clear that

personal identification, possibly involving biometrics, is a key element here. The challenge will be to protect the integrity of the process without burdening this ***right*** to vote in ways that may decrease registration by eligible voters.

Making Sure Only Eligible Voters Register

The 14th, 15th, 19th , 24th, and 26th Amendments to the U.S. Constitution identify eligible voters as all citizens 18 years of age and older who have not been convicted of a disqualifying crime. Implicit in these Amendments and the NVRA, and explicit in voting codes, is the additional requirement that each citizen is eligible to register only once. Establishing that you are a citizen at least 18 years old cannot be done directly by biometric identification. This requires trusted source documents, like a certified birth certificate or a passport. If these source documents were linked to a biometric record, which they are not, positive biometric identification could be used to establish the connection of the presenter to the presented source documents. Driver's licenses in the States of Texas and Georgia display encoded fingerprints and could be used to link a presenter to an identity through biometrics, but they are not proof of eligibility to vote and merely transfer the original identification burden to the driver's licensing system. In the absence of biometric data on passports or birth certificates, biometric identification cannot be used to establish my eligibility to vote.

Each citizen is allowed to register only once and in one jurisdiction: "one voter, one vote". In registering to vote, I declare my previous registration, if any, so that I can be removed from the voter roles of my previous jurisdiction. Negative biometric identification could be used to determine if I am previously registered in the current or other jurisdictions, preventing voter fraud through multiple registration of the same voter.

Under the 14th Amendment, citizens can lose eligibility to vote for conviction of some crimes. In registering to vote, I attest that I am not someone who has lost eligibility through conviction of a disqualifying crime. The National Association of Secretaries of State has recommended that a task force investigate the creation of a national clearinghouse of names of disqualified voters to allow the cross-jurisdictional enforcement. This negative biometric identification could be done with fingerprinting because fingerprint records are available on those convicted of disqualifying crimes.

In considering biometric identification for preventing multiple registrations or for preventing registration of disqualified voters, recall that such "negative" identification must always be mandatory for all enrolling in the system. In other words, enforcement of "one-voter, one vote" and disqualification provisions using biometrics would require the mandatory biometric measurement of all registration applicants. In the case of preventing registration of those disqualified by criminal record, fingerprinting of all registering voters would be required. This would not only require specialized equipment[2], it would place a burden on the entire process for all registrants to deter the activities of a very few. Further, mandatory fingerprinting might be considered a de-

[2] There are "ink-less" fingerprinting systems available, but there is no evidence that such systems can be successfully used, except by forensic experts, to acquire fingerprints suitable for electronic systems.

terrent to registration by those who mistakenly believe that fingerprint databases on minor traffic offenders exist through driver's licensing systems.

Burdening the entire process should be considered only if there is adequate documentation of a clear need. We know of no documented studies on a national basis showing massive fraud through multiple registrations or through the registration of criminally disqualified voters. In short, it is not clear that there is a currently justification for adding mandatory "negative" biometric identification to the voter registration process.

Making Sure Only Registered Voters Vote

Another identification problem faced in the voting process is the positive identification of voters at the polls. Can the poll workers be certain that people appearing at the polls are who they claim to be? The current solution to this problem in many jurisdictions is to have voters announce their name aloud; the concept being that poll workers or other voters present could challenge false claims of identity. Voters are also required to sign a roster. If a voter's identity is challenged later, the roster signature can be compared to that given at registration.

This process could be strengthened in a number of ways. Voters could be asked at the polls to supply additional information given at the time of registration, such as their address or birth date. Voters could be asked to present identification documents, such as a driver's license, birth certificate or utility bill. Voters could be asked to bring to the polls mailed election materials showing name and address. Or voters could supply biometric identification.

This use of biometrics for positive identification could be done on a voluntary basis. Jurisdictions wishing to give voters this option would allow those requesting biometric identification to record a biometric measure when they register. This would require special equipment at the registration sites, as well as at the polling places. It would require the centralized storage of these measures by the jurisdiction. It would also require the transmission of the biometric measures between the jurisdiction and the polling places on election day.

Of all the methods we've listed here for strengthening the process of identifying voters at the polls, biometric identification would require the most additional equipment and cause the most changes to the current systems. However, it would also be the method hardest to defraud. We have, again, seen no documented evidence showing widespread, national problems with voter identification at the polls. If there is a need to strengthen the system in a particular jurisdiction, it seems sensible to start with other less secure and less costly methods of voter identification. Only after these methods prove to be insufficient, or there is a general demand by the voters to allow substitution of biometrics for these methods, could a practical case be made for biometric identification.

Absentee, Nomination and Petition Applications

The identities of voters applying for absentee ballots, petitioning the government or nominating candidates are currently verified by comparing the signatures on these documents to signatures in the voter registration

rolls. This labor-intensive process is often aided by electronic "election signature retrieval" systems. Handwritten signatures from voter registration documents are optically scanned into a computer system. Then, election officials can electronically recall these signatures to compare them to those on petitions, absentee ballots and nomination forms. The actual comparison of the signatures is done by human eye.

This process of comparing signatures could be automated. Computer programs for comparing written signatures currently exist in laboratories, but are not currently commercially available. These systems require no special hardware and are different from commercially marketed "dynamic signature verification" that require special pens and tablets. Even if quite crude, this form of biometric identification could successfully reduce the human workload by automatically accepting the signatures that are clearly legitimate or at least very good forgeries: the same signatures that would be easily accepted by human examiners. Only signatures that are not obvious matches would require a human decision. We believe that such automated signature matching could be profitably integrated into current electronic signature retrieval systems.

Other Applications

We can imagine more elaborate uses of biometrics for prevention of "chain balloting" or to allow completely anonymous voting. Chain balloting is a method for corrupting document-ballot elections. A campaign worker gives the complicit voter a pre-marked ballot before he/she enters the polls. At the polls, the voter conceals the pre-marked ballot and is given a blank ballot. The pre-marked ballot is cast and the blank ballot surreptitiously returned to the campaign worker after leaving the polls. The campaign worker marks the ballot for the next voter. In 1992, about half of the States using a document ballot had procedures in place to prevent chain balloting.

Biometric identification could be used to print a biometric identifier on the ballot stub when the ballot is issued. The biometric measure on the stub could be compared to one taken from the voter when the vote is cast. The stub would be given to the voter so that no biometric record of the voter would remain at the polls after the voter has left. This application would require the mandatory biometric measurement of all voters.

In theory, completely anonymous voting could be accomplished by registering volunteering voters under a biometric identifier. Eligibility at registration would be ascertained using current methods and registration records would include the voter's name. Only the voter's biometric identifier, however, would be sent to the polls. At the polls, voters would present the biometric identifier in lieu of announcing a name. This extreme application would significantly alter the current system of publicly releasing the names of those who have voted.

Internet Applications

In 1999, the State of California created an "Internet Voting Task Force" to study the possibility of casting votes over the Internet. The task force found that one of the obstacles to Internet voting would be the identification of the person casting the vote.

The problem of identification of Internet voters is one of both positive and negative identification. Negative identification would be required if we wished to prevent multiple registrations of the same person. Positive identification would be required to identify the person casting the vote as the registered voter.

As discussed, negative identification must be mandatory for all voters. In the case of Internet voting, multiple Internet registrations could be prevented by the mandatory biometric identification of all Internet voters at registration. This would not require mandatory identification of non-Internet voters if we were willing to allow for the possibility of fraud through both Internet and paper registration of the same voter under different identities. Internet registration with the submission of a biometric identifier could not be securely done over the Internet, but would require "in person" registration and the collection of the biometric identifier by trained and trusted persons This identifier would be placed in a database under the control of the jurisdiction. Upon verification that the registering voter is not already in the database, a voter ID number, code or PIN could be issued. Biometric identification and specialized hardware at the time of voting would not be required for negative identification.

Positive identification by Internet voters using biometrics would require that biometric measures be previously registered "in person" with the jurisdiction and would require standardized biometric collection hardware and software on the computer used for voting. Positive biometric identification might be used on a voluntary basis to replace other types of PIN or password identification. An added problem is the occasional failure of all biometric techniques to recognize properly registered users. "Provisional" voting would have to be allowed in cases where the voter's submitted biometric measure did not seem to match the registered measure.

In short, biometric identification could be an important adjunct to Internet voting, but would not solve all identification problems inherent in Internet voting.

Conclusions

In this paper we have looked at specific applications of biometric technologies to the voting process. We can conclude that biometric identification could be effectively used, even on a voluntary basis, to detect and deter voting fraud. Biometric identification, however, is not a "silver bullet" capable of solving all problems of voter identification without any undesirable side effects. Use would require fundamental changes in the way we register voters and would necessitate the creation of government-controlled databases of physical and behavioral characteristics of at least some voters. Although such databases pose no threat to the privacy of voters, the process could be seen as an additional burden on the registration process. We would need to carefully consider the potential impact of such changes on the competing requirements of the National Voter's Rights Act of 1993 to both enhance voter participation and to protect the integrity of the electoral process.

Other titles in our Innovations series include:

- Vol 1: The Voting Authority Card
- Vol 2: Optical Scanning Technology for Purposes other than Ballot Counting
- Vol 3: Election Signature Retrieval Systems
- Vol 4: Using NCOA Files for Verifying Voter Registration Lists
- Vol 5: Agency Voter Registration Programs
- Vol 6: Motor Voter Registration Programs
- Vol 7: Mail Registration Programs
- Vol 8: Election Document Retention in an Age of High Technology
- Vol 9: Early Voting
- Vol 10: Ballot Security and Accountability
- Vol 11: All-Mail-Ballot Elections
- Vol 12: The Electronic Transmission of Election Materials
- Vol 13: Simplifying Election Forms and Materials
- Vol 14: Recruiting Poll Workers
- Vol 15: Ensuring the Accessibility of the Election Process
- Vol 16: Using the Internet in Election Offices
- Vol 17: Acquiring Election Systems and Equipment

For information about other

Innovations in Election Administration

contact

Office of Election Administration
Federal Election Commission
999 E. Street, N.W.
Washington, D.C. 20463

Toll Free	**800.424.9530 (option #4)**
Direct	**202.649.1095**
FAX	**202.219.8500**
e-mail	**bkimberling@fec.gov**

FEDERAL ELECTION COMMISSION
WASHINGTON, DC 20463

OFFICIAL BUSINESS
Penalty for Private
Use, $300

Bulk Rate Mail
Postage and Fees Paid
Federal Election Commission
Permit Number G-31