Bio-Metrics to safeguard society

A White Paper on Bio-Metrics by Thomas Bronack

I have been intensely watching the candidate campaigns for the presidential election, along with paying close attention to the terrorism problem faced by most countries, and believe the best method to guaranty the safety of America and its people is through a Bio-Metric Smart Card Identification system that would guaranty that people are who they claim to be. I have used this approach in an electronic voting system I designed (patent pending) and believe the approach would solve a multitude of problems associated with identifying and tracking people who could pose a problem to our society. The system works by obtaining personal bio-metric information (eye scans, facial recognition, finger prints, etc.) and down-loading the individual's bio-metric information into an electronic Chip on a Personal ID Smart Card to produce a "**Personal Identification Smart Card**" for the individual. This ***eCARD*** can be scanned and compared with a full range of bio-metric information, so consider it a **Universal ID Card** that can satisfy business, government, and personal needs. The Universal ID Card will satisfy and exceed the requirements defined in the "**Real ID Act**" of 2005, which all States have to adhere to by January 22, 2018.

The ***eCARD*** will validate that a person is who they claim to be by comparing the bio-metric information stored on the individual's card with bio-metric information taken on the spot. If a match is achieved, then the person is verified as being who they claim to be. But we don't stop there because the bio-metric information is compared against the individual's initial data base entry to validate their identity further and then the Voter Data Base to insure that they have not voted in this election somewhere else. We can also perform searches of other system data bases to insure that the individual is on the "Eligible Voter List" and does not have an outstanding criminal "want or warrant". If the individual fails any of these tests, a message is sent to the physical security group protecting the voting station before the individual can extract their card from the Smart Card Holder. Security will then detain the individual for questioning and possible prosecution, while the system will provide an Audit Trail of the individual's activities (including pictures) for use in documenting the crime and prosecuting the individual. Finally the individual's ***eCARD*** will be retained by the guard as evidence.

The guaranteed proof of identity provided by the Personal Identification Smart Card can aid in many ways, for example:

1. **Proof of Identity** can be used to support applications for many other services from VISA Application through Motor Vehicles, to Requests for Social Security and Family Services, all without violating current privacy laws.
2. **Law enforcement** can be greatly aided in quickly identifying an individual and their threat level, so that a speedy reaction and apprehension of a criminal / terrorist posing a major threat can be accomplished.
3. **Adding** a **GPS system** to the ***eCARD*** can be used to track personal activity when a legal warrant is issued, or in cases of civil unrest when you want to identify and track felons fleeing a scene after committing a major crime.
4. **In essence**, the Personal Identification Smart Card will provide the fastest method for identifying and reacting to individuals committing crimes, posing threats, or other acts that could hurt the country and its Citizens – along with identifying and tracking aliens from the time they reach our shores throughout the activities they perform while here.
5. The ***eCARD*** also meets and exceeds **Real ID Act** requirements, mandating adherence by all States no later than Jan. 22, 2018. Should a State not meet Real ID Act requirements individual access to commercial flights, and a wide-range of government and private sector services will not be granted.

An example of how this approach would help is if the airport in Brussels had a Facial recognition system they would have spotted the bombers prior to the bomb explosion they could have used trace information to determine their activities prior to, during, and after their criminal act, accumulating information essential to prosecution and identifying associates. **They didn't, but we could, and that is the best way to lead – by example.**

It is my belief that **modern technology should be applied** to many of the antiquated systems used by our government and law enforcement agencies by employing Smart Cards with chips to verify / validate individuals and track activities of those individuals considered a threat, or are under legal court orders to surveil or restrict movement.

This paper provides **some examples** of my concerns and how we could produce a system that would overcome problems related to crimes committed by individuals, but I am totally prepared to discuss these issues and I can make myself available should you want to pursue these issues.

The Problem – we can't positively identify people

The use of Bio-Metrics on a Smart Card can solve a wealth of problems related to identifying and tracking people and to authorize the individual's right to receive services, including:

1. Passport
2. Alien Identification Card
3. Driver's License
4. Welfare and Social Services
5. Voter ID Card
6. Health Care, and many more.....

The Solution – Use Bio-Metrics to identify and track people

You can also utilize a Smart Card System (SCS) to identify an individual via Bio-Metrics, including:

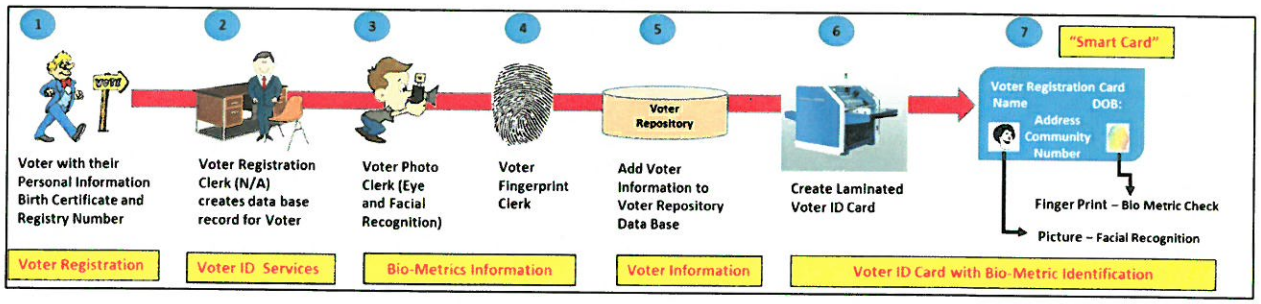
1. DNA,
2. Eye Scan,
3. Finger Print
4. Facial Recognition
5. Voice Recognition,
6. GPS Location Chip, etc.

Insisting that an individual **prove who they are** prior to allowing them to Vote, Receive a Driver's License, Obtain a VISA or Passport, Fly of a Commercial Airline, or Receive an Alien Card is presently the norm, but adding a Smart Chip to the process would go a long way towards solving many other problems being addressed during the current election process – "We must provide better protection over our borders", "It is imperative that we track immigrants or suspects to insure the safety of our country and population", etc.

What is missing is **a solution that can address all of these problems** and more, without forcing the government to implement a new and expensive system. I am suggesting a solution that can work right away in its initial phase and grow over time to include multiple checks covering a full-range of problems currently being voiced by the people and those seeking public office. My concept includes creating a bio-metric data base of records for individual's that can be compared locally to perform Identification and remotely to perform Vetting, authorization, tracking, and reporting.

My recommendation is as follows.

How it works



Although this is a picture from an electronic voting system, it can serve as an example of my concept because it shows the steps necessary to obtain personal bio-metric information and create a Personal Identification Smart Card. The process would include:

1. **Individual** enters location to obtain a Smart Card Identification for Voting, Driver's License, Passport, VISA, Immigration Services, Alien Identification, TSA, Social Security Benefits, Welfare, etc. (the list can go on until all requirements are met).

2. **A clerk** assists the individual complete the paperwork required to prove they are who they claim to be (background checks can be performed if necessary, but certainly Picture ID, Payroll Statements, Bills Mailed to their address, etc. would be needed to support their claim). This information is used to create a data base record for the individual as a foundation record (Parent) that would be added to as more processes are completed, but as of this point in time we have a documented individual claiming to be someone specific.

3. Stage three is when **Bio-Metric information is obtained** from the individual, for example: DNA, Eye Scan, Facial Recognition, Finger Prints, etc. At this point we have the paperwork submitted by the individual and the bio-metric information associated with the individual so a comparison can be made to prove identity.

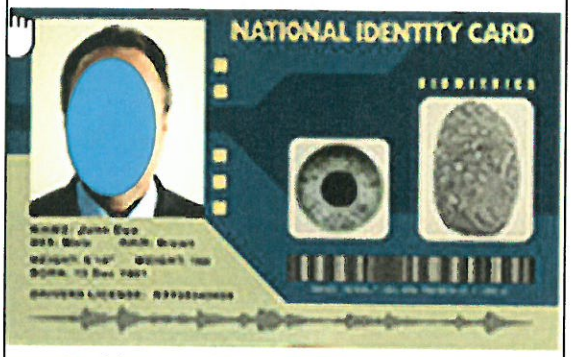
4. The **bio-metric information is checked** to insure it has been accurately taken and meets the parameters of the bio-metric equipment being used to scan, read, and process the bio-metric data. Today Smart Cards with chips are inserted into a slot added to the normal charge card scanners. The Smart Card is inserted instead of swiped and must be retained in the machine until the transaction is completed. This is an important issue related to a Smart Card and will allow for apprehension of criminals while in the act of committing a crime, and/or the confiscation or erasure of information on the chip to eliminate duplication of thefts or criminal acts associated with the Smart Card. Just think about the implications behind that feature, while remembering the size of the equipment needed to read and process the Smart Card (a small investment indeed – think Apple Square).

5. The individual's Smart Card **Contact information** would be used to populate their data base "**Parent**" record, while the individual's **bio-metric information is stored as a Child Record**. You could also have **Cousin Records** that are associated with a Child Record but not a parent (think "Known Associates"). Having a Parent / Child record relationship will allow the addition of information to the individual's identification that could be generated by other government offices and examined without knowing who the information belongs to unless a match is made that would grant legal access through a court order or approved process.

6. In this stage, **the Bio-Metric information has been verified locally and validated** through remote systems (like Motor Vehicles Driver License ID System, Criminal Records maintained by the FBI / CIA, Voting Activity for current election and past archives, or any other system needed to fully Vet an individual). At that time it is safe to generate a Bio-Metric based individual Smart Card Personal ID and store the individual's bio-metric information on the Smart Card chip. A safeguard associated with this process would be to deny a Voter ID Smart Card to Felons who are not allowed to vote by law. Other warning flags, or restrictions associated with this individual (no-fly list, civil warrant, parking tickets, etc.) can be accumulated over time and related to the individual as a Child Record, which would be displayed if the card is scanned by law enforcement or within a vetting process.

7. Once the individual is totally vetted, an **Identification card will be generated**, laminated, and provided to the applicant. This entire process can take as little as 30 minutes, but will probably take longer in the beginning due to a learning curve and equipment weaknesses.

What a Bio-Metric ID Card Looks Like



Facial Recognition, Eye Scan, Finger Print, and Voice Recognition

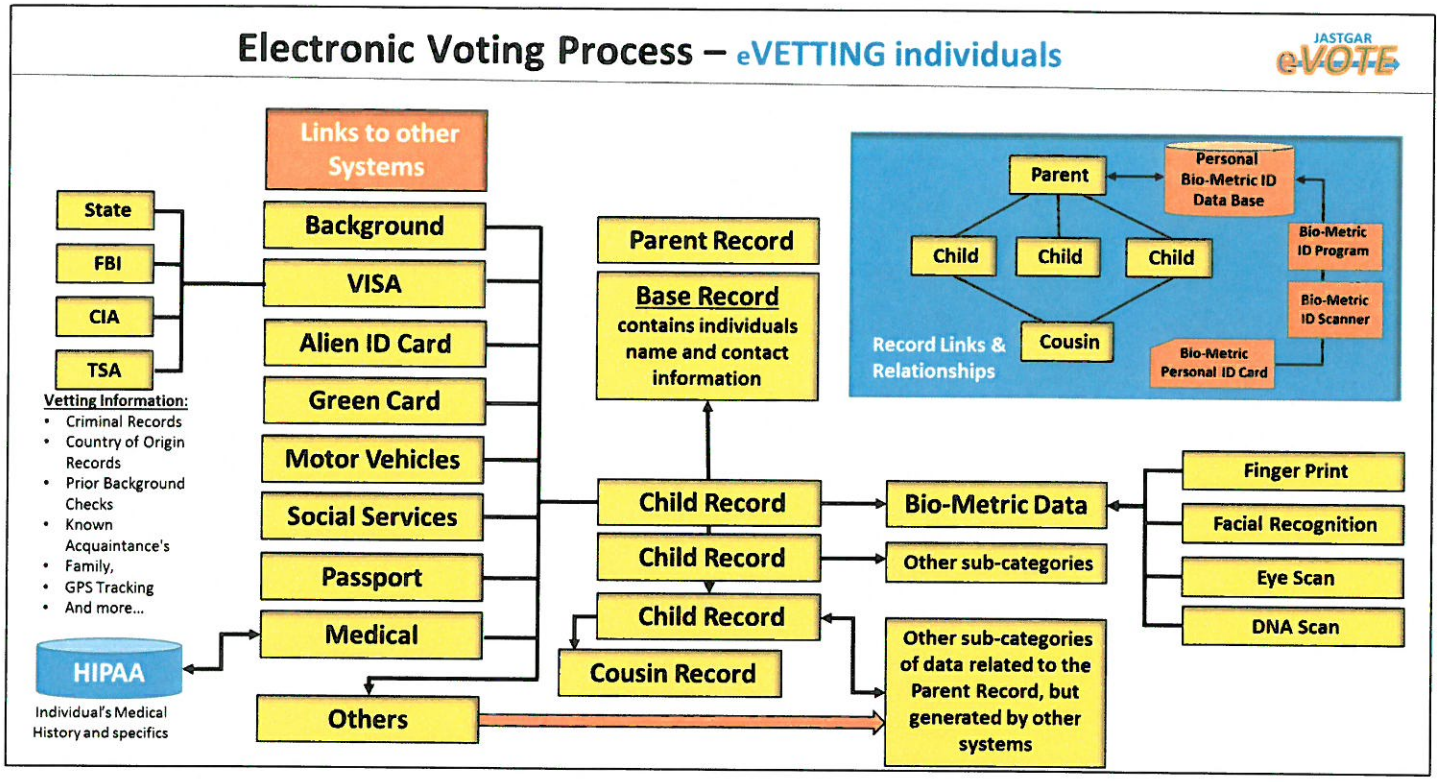
The **Data Base Relationship** looks like the picture below. As you can see, other systems can link to the Individuals Child Record to scan Bio-Metric information, but not the Parent Record unless a match is made and legal authority granted.

All government and authorized systems can also generate sub-categories of information that can be appended to the Parent Record as Child Records. This is **very efficient**, because if the individual changes addresses or personal information the change is performed once and all other systems will have access to the updates so they can use that new information for mailings, emails, and other communications to the person defined in the Parent Record. This one change for many systems approach is most efficient and will result in fewer data entry errors, especially if you have the person represented in the Parent Record perform the update themselves (think **Profile maintenance**). Changes to an individual's location and status information should also be vetted to insure accuracy and aid in locating the person being sought.

The **Cybersecurity Information Sharing Act of 2015** was introduced recently to encourage security information sharing between the government and private sector in order to grow and improve security information availability and better protect private and public sector enterprises. This law and the **Real ID Act of 2005** could be the foundation used for pursuing the recommendations stated within this document for creating a **Universal Smart Card Personal ID**.

The Data Base Record structure creates a Parent Record that links Child Records and even Cousin Records into a Relationships (Blue Box Below) showing the Parent, Child, and even a Cousin Record that could be used to identify associates. The Data Base is generated, read, maintained, and deleted through the **Bio-Metric ID Program**, and remote access to authorized individuals would be via a **Bio-Metric Scanner** that reads the Bio-Metric Personal ID Card while it is inserted in the Bio-Metric ID Scanner (the card remains in the scanner until the operation is completed, thereby guarantying apprehension of violator or disablement of the Smart Card so it could not be used to commit further crimes or violations).

The Data Base Relationship



Now that we have the **person's identity and location**, along with a range of status information, it will be easier to locate and track individuals should the need arise. This system provides law enforcement with a very strong tool, especially with the aid of GPS information transmitted via the card's chip and the documentation that can be generated to support prosecution.

The **identification process** would be to insert the Bio-Metric Personal ID Card into a Bio-Metric ID Scanner that is connected to the Bio-Metric Program, which can access the Personal Bio-Metric Data Base (see above picture – upper right blue box diagram). The Bio-Metric ID Program would search the Child Records for anomalies, the Cousin Records for Associates, and eventually the Parent Record for identification should it be warranted. This process would produce an all clear, warning, or arrest command to the Law Enforcement Officer on the spot (total elapsed time is in seconds), so that an apprehension can be made if directed.

The card holder will find their new card helpful as well, because the new card and chip can be used for all systems linked to it (i.e. voting, motor vehicles, TSA, Justice Department, Treasury Department, Homeland Security, State Department for a passport, etc.). The smart card will also be able to support local verification and remote validation of individuals wanting to participate in an on-line caucus or other such electoral activity. They could be verified via home scanner or smart cell phone (think finger print scanner on an iPhone) and allowed to submit their ballot in a caucus. Once submitted the individual would be entered into a "Chat Room" associated with the candidate they submitted their ballot for (say Donald Trump). In the Chat Room, the individual would respond to questions and try to sway others to agree on points they would use to justify their vote for the candidate. After the Chat Room session is completed, people agree on the candidate and supportive information, they submit their vote (everyone's name and contact information is already known from their Voter ID Smart Card without the need of a paper ballot). Their results are added to the results from all Chat Rooms for a candidate, along with their points about why their candidate is the best person to elect. Now is when

the caucus starts, because the Chat Room totals and points of justification are submitted to the other side's chat room results and a discussion is conducted electronically until the final voting is completed.

This process would be very easy to accomplish from the comfort of an individual's home, without clogging roads and potentially getting into a car accident. Also, telecommuting has become common place so why not take advantage of it. No problems with running out of ballots, because they are electronically generated. The ballots are completed on-line so they are easily readable. They could even be translated from one language to another (for example from English to Spanish or Chinese). And the costs of renting locations to conduct caucuses would be greatly reduced, or eliminated.

Once this process has been completed and the final votes submitted, the tally could be calculated in seconds (near real-time) and made public. Of course, checks and balances can be applied to the voting process, but you would never see people rushing into a caucus and submitting recently printed pieces of white paper (instead of blue for example) into a box for counting – no verification needed and so easy to commit fraud / corruption.

As you can see, my basic premise is that **we have the technology today** to address these problems and more. As we accumulate safeguarded information we can better detect fraud, corruption, terrorism, criminal activities, and illegal aliens and many more illegal activities – while protecting people better.

If a "**Cashless Society**" was created, where transactions were performed via Smart Card, it would be so easy to **spot fraud and eliminate identity theft** that the reluctance from the population for using this technology would be reduced to a point of virtual elimination. The Patriot Act and Dodd Frank would be satisfied easily through this process as well as the Sarbanes Oxley Act (SOX).

I am a strong and loyal supporter of our country who has accumulated a lot of knowledge throughout my 45+ year career in Information Technology (IT) - started with IBM and now working on a system to capture cyber-crimes and technology threats in near real-time. I believe this approach could be of value to **protect the country's population and our society**. I am offering my services in any way that could help.

I welcome all comments and recommendations for improvement and can be reached via email at bronackt@gmail.com, or phone at (917) 673-6992 (email preferred).

Sincerely,

Thomas Bronack

Thomas Bronack

Email: bronackt@gmail.com

Phone: (917) 673-6992