Biometric Identification:
A Benefit-Risk Analysis of Israeli Applications
Biometric Identification:
A Benefit-Risk Analysis of Israeli Applications

Authors:
Jay Levinson
Karine Nahon
Avi Domb

This paper is an output of PACT’s Work Package 7

Acknowledgement: The research presented in this paper was conducted in the project “PACT – Public Perception of Security and Privacy: Assessing Knowledge, Collecting Evidence, Translating Research into Action”, funded by EU FP7 SECURITY, grant agreement no. 285635
Biometric Identification:
A Benefit-Risk Analysis of Israeli Applications

Jay Levinson
Karine Nahon
Avi Domb

Abstract: This paper discusses the benefits and problems inherent in biometric identification, first from a theoretical perspective, then with examples from the Israeli experience. The differences between civilian and security considerations are highlighted.

Keywords: Biometric, identification, passport, privacy, security

Short biography of the author/s:

Jay Levinson, after retiring from the Israel Police, has published many books and articles. He has written extensively about professional matters including a history of Disaster Victim Identification in Israel. In the 1990s he served for five years as the Chairman, Interpol DVI Standing Committee. Levinson holds a Ph.D. in Near Eastern Studies from New York University. He is currently an adjunct professor at John Jay College, a research assistant at the Hebrew University of Jerusalem, and a member of the editorial boards of Crisis Response and Disaster Prevention & Management.

Karine Nahon is an associate professor at the Information School of the University of Washington, and the Lauder school of Government at the Interdisciplinary Center In Herzliya, Israel. Her research focuses on information politics and policy. Karine is the author of the book, “Going Viral” (with Jeff Hemsely), and her papers have been published in top-tier journals. Karine is also publicly active on topics of technology and society. She serves as a member of the Israeli CIO Cabinet, and a board member of NGOs that promote transparency such as the Freedom of Information Movement, Wikimedia and the Workshop for Open Knowledge. More can be found on her website: http://eKarine.org

Abraham J. Domb is a Professor for Medicinal Chemistry and Biopolymers at the Faculty of Medicine of the Hebrew University of Jerusalem. He earned Bachelor degrees in Chemistry, Pharmaceutics and Law Studies and a PhD degree in Chemistry from The Hebrew University. He did his postdoctoral training at MIT and Harvard University, Cambridge USA and was R&D manager at Nova Pharm. Co. Baltimore USA during 1988-1991. Since 1991 he has been a faculty member at the Hebrew University full professor since 1999). During 2007-2012 he headed the Division of Forensic Science at the Israel Police. His current areas of interest include: biopolymers, drug delivery systems, bioactive polymers and forensic sciences.
Biometric Identification:
A Benefit-Risk Analysis of Israeli Applications

1. Introduction

This paper explains the decision making process behind the establishment of biometric databases, then it concentrates on the current situation in Israel regarding active biometric files, discussing their effectiveness, efficiency, and potential risks to privacy. The paper compares civilian and security uses of biometric databases. The authors argue that there are intrinsic problems in the maintenance of biometric databases, and an even greater danger exists when ostensibly harmless databases are combined. The study aims to use the Israeli case as a catalyst to encourage exchanges between practitioners and scholars about the questions and issues that need to be raised in countries implementing biometric databases.

There are different stages in the decision-making process of building a biometric program: conceptualization, goal definition, identification of constraints, proposal, tentative approval, testing, evaluation, approval, and implementation. The latter stage includes data collection, retention, and retrieval. Data security and privacy begin at the testing stage, when a proposal is often tested with real personal information. Privacy and security risk analysis are of key concern in this paper.

The first four parts of the decision-making process are highlighted in discussions.

| 1. conceptualization |
| 2. goal definition |
| 3. constraints |
| 3a. public acceptance |
| 4. proposal |
| 5. tentative approval |
| 6. testing |
| 7. evaluation |
| 8. approval |
| 9. implementation |
| a. data collection |
| b. retention |
| c. retrieval |
| 10. re-evaluation |

2. Discussion

Biometric identification is the procedure of identifying people by their physiological and behavioral characteristics. The most common examples are fingerprint\(^1\) and palm\(^2\) prints, odontology\(^3\).

---

Hence, some appear more often as court evidence.


3. Framework of Analysis

A properly designed biometric identification program involves numerous stages in the decision-making process. This framework suggests considerations and questions at each stage.

3.1 Conceptualization

One must pinpoint the problem to be resolved. An example of a problem to be resolved would be the accurate verification of the identity of a person wanting to cast a ballot at a polling station to insure that only the appropriate voter is allowed to participate in the electoral process.

3.2 Goal

Defining goals is the stage following conceptualization. At the polling station the goal is to verify that the potential voter is the “John Doe” who is eligible to vote in that station, not to identify him amongst all persons in the country. Clear goals are critical; the analysis and ramifications of a verification phase (1:1) versus an identification phase (1:n or m:n) are different.

A difference also exists between civilian and security goals. A civilian goal is to verify the identification of the potential voter against the voting list based upon identification that he presents. It is not to establish the identity of the potential voter from a databank of the entire population. If fraud is established, the goal is transformed from a routine civilian verification into a police security issue of true identification.

A murder investigation is another civilian example. The police or pathologists not only verify and also identify the perpetrator based on evidence left at the crime scene. If the victim is totally anonymous, then he must also be identified.

3.2.1 Fraud Prevention

Accuracy must be part of any goal. Fraud, a flaw in accuracy, has been experienced throughout the world. There are two general categories of fraud relevant to this paper --- (1) identity

---

9 “…[posture] generally include[s] movements of the fingers, hands, arms, face, head, and body. See Teng, Wei-Guang; Hsu, Meng-Chin; Hsu, Yu-Yun; Hou, Ting-Wei. “Posture Identification with Markerless Commodity Devices.” Advanced Science Letters, Volume 9, Number 1, April 2012, pp. 399-405(7)
12 Although all of these biometric categories are individual, some are more easily measured than others. Hence, some appear more often as court evidence.
13 In mathematical terms, a 1:1 comparison is required rather than 1:n or m:n.
document fraud and (2) identity theft, the two most common general types of fraud. Both are criminal acts.

<table>
<thead>
<tr>
<th>Identity Document Fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Genuine documents that are stolen when blank then “issued” illegally.</td>
</tr>
<tr>
<td>• Illegally printed documents</td>
</tr>
<tr>
<td>• Altered documents</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Identity Theft</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Genuine identification (documents issued legally but based upon illicit supporting documentation)</td>
</tr>
<tr>
<td>• Fraudulent data or documentation in the name of another person.</td>
</tr>
</tbody>
</table>

The most difficult method of fraudulent identification to detect is a genuinely issued document in another name --- sort of the “Man Who Never Was.” Known tactics are numerous. One is to obtain the genuine birth certificate of a person deceased in a far-away city, then to use that as the basis of acquiring other genuine documents.

There have also been cases of genuine documents issued on the basis of totally forged or stolen supporting papers.

One does not only react to fraud; one also tries to prevent it. Over the years as technology has advanced, virtually all countries have introduced new and sophisticated printing, photograph, and lamination techniques to insure document security. These techniques help thwart numerous crimes, and they do not directly address information privacy concerns.

As a goal it would be reasonable to devise even newer methods of document security to prevent forgery, and to reexamine document issuance procedures so that only authorized recipients receive papers from birth certificates to passports, from a driver’s licenses to credit reports.

Another goal is to ensure that a document does, in fact, belong to the person presenting it.

Public acceptance is also a constraint. In a democratic society not all effective programs will be supported will be supported by the public.

Many identification problems are shared by both the government and private sectors. A common commercial example is verifying the identity of a credit card holder. There is a basic tendency to allow government to collect more information about us than we would allow in private hands. How can we keep proportionate control within the bounds of public acceptance?

In the credit card example the real “John Doe” can have extreme difficulty proving that he did not make certain purchases based upon a credit card issued in his name. The credit card might have

---

15 Israeli statistics are not available, but this is a common problem in many countries abroad.
been issued on the basis of biometrically supported identification (e.g., driver’s license or identification card), but private companies do not have the capability of realistically checking that biometric data when issuing or using the credit card. If such data were available for credit card issuance, it would mark a spiral of privacy concerns.

Nor are physical credit cards necessarily required to make purchases. Persons assuming the identity of others do not necessarily need to go to the trouble or expense of producing cards. In today’s technological world telephone and Internet transactions require data and not necessarily the physical card.

3.3.1 How Much Information should be Collected?

When identity verification is the goal, how much information is necessary and should be collected? Excessive collection can well be an intrusion into personal privacy. On the level of privacy Andrew Clement of the University of Toronto has used an interesting term, “Proportionate Identification.” That is to say that a source requiring personalia should only be given what is required. For example, a bartender should be given proof of age on an authoritative document associated with the bearer, but he need not know place of residence. A postal employee needs to know a person’s address, but not necessarily his age. Consider the voting example. The potential voter has to allow his identity to be verified, not established from a national registry. Only when there is criminal intent in misrepresentation and fraud is the goal changed. Then there a need for a more extensive database.

3.3.2 When does “Much” become “Too Much?”

“Big Data” is a relatively new term denoting “a collection of data sets so large and complex that it becomes difficult to process using on-hand database management tools or traditional data processing applications.” This should not be taken in absolute terms of what equipment and manpower can theoretically be procured to maximize data management. More practically, goal definition should take into consideration problems of Big Data weighed in real terms of existing or reasonably purchased database management tools. This, however, is a theoretical consideration. Goals of extremely large databases should sound an alarm in terms of real need versus citizen privacy. One pragmatic step is to set controls on database size as early as the goal definition stage.

3.3.3 Which Information should be Collected?

Realizing that there are reasonable limits to data collection, in terms of biometric data for widespread practical application five characteristics of data must be considered. These are categorized by Jain et al.: Universality (traits found in every person), Uniqueness (different with individuals in the relevant population), Permanence (not changing over time), Collectability (ease of collection), Performance (technology of collection and sorting), Acceptability (popular acceptance of the method and its application), and Circumvention (difficult substitution or forgery). A decision about the type of biometric data to be collected should involve a biometric

---

20 http://en.wikipedia.org/wiki/Big_data
22 It is, of course, recognized that few biometric features will be common to all persons in the general population. There will always be an exception such as a person who cannot be fingerprinted due to a physical condition such as an amputation, burn, or a bandage.
technology that can apply these five traits. However, bureaucratic reality presents further constraints to consider in the decision-making process, such as cost and rapidness.

### 3.3.4 Information Retention

A corollary to information collection is retention. Information retention should be defined as part of goals, which will later be applied to proposals. The longer information is kept, the more vulnerable it is to unauthorized access. Here again there are differences between civilian and security purposes. In a civilian context there is a basic question if biometric data are to be retained after their use has expired. An example would be the retention of a DNA sample after the resolution of a paternity dispute. For security goals there are advantages in retaining biometric files. A case from the United Kingdom illustrates the point.

In the case of S. and Marper v. the United Kingdom argument was made to the European Court of Human Rights that British authorities retained fingerprint, communications, and DNA records after the two persons had been acquitted of the crimes of which they were accused. The police denied the request of the two individuals that their records be destroyed.

The background to the police position is interesting. Testimony was presented that 6000 DNA samples that might have been destroyed under non-conviction guidelines were linked to 53 murders, 33 attempted murders, 38 sex offences, 63 aggravated burglaries, and 56 drug cases.

In other words the United Kingdom experience clearly shows that there can be significant benefit derived from retaining ostensibly “useless” data. The primary financial cost involved is in collection, not retention and retrieval. The basic issue is not monetary cost versus police utility. The issue essentially involves privacy concerns and potential police operations.

Similar to the UK case, numerous “cold cases” have been solved using data on file in other countries.

Partial DNA matches provide an interesting issue. Sometimes DNA samples on file do not single out the perpetrator of a crime (exact match); the eventual identification is based on one of his relatives (partial match). This is the case, for example, of Lonnie David Franklin, Jr. who was arrested in Los Angeles for serial murders based on partial DNA matches with his son, a suspect in a felony weapons case. It was reasoned that the murderer was related to the son; that premise directed the investigation. If the son had theoretically been cleared and his records deleted from police files, Franklin would not have been caught.

Moving away from criminal cases, one should again examine the voting example. After a person shows that he is a citizen eligible to vote, is of appropriate age, and lives in the polling district,

---

23 For a list of countries retaining biometric information databases see Israel Supreme Court 1516/2012, 23 July 2012, Government Response.
25 This is true in police terms in most countries, when an extensive network of evidence technicians and investigators has been established to collect information. In the civilian framework of the Israel Ministry of Interior the opposite is true --- the costs of retention and retrieval are greater than collection. This is one of the many differences between civilian and security considerations.
should that information be retained? The answer to that question lies in goal definition. How to implement it is a proposal question.

3.3 Constraints

Not everything that is theoretically desirable is, in fact, possible. In the bureaucratic world the constraints of finances, manpower, and public opinion are common concerns. Regarding biometric identification in a democratic country there are also technical and ethical constraints.

Bureaucracy very much stresses cost effectiveness. Finances are an issue at all stages (equipment purchase, staff training, database management, project maintenance, etc.). These costs must be weighed against the scope of the problem, its severity, and alternative solutions. Government funding is not endless, even when budgets are generous. In the end programs must be shown to be fiscally responsible.

For general application of biometric data in functions such as border control, access control, or police on-the-street inspection, any biometric method if chosen for implementation must be rapid (e.g., fingerprints or iris / retina). DNA, for example, is virtually\(^{28}\) definitive, but with today’s technology it is time consuming (even when compared under standards lower than those needed for court evidence\(^{29}\) the test takes 75 minutes\(^{30}\)), hence not at all practical for many applications. The IntegenX RapidHIT™ 200 Human DNA Identification System, validated per SWGDAM (FBI) guidelines, has been fielded in mobile situations,\(^{31}\) but its 90 minute reaction time is more appropriate for crime-connected use rather than routine biometric identification verification.

3.3.1 Public acceptance

Proposals are not accepted by the public are very hard to put into effect in a democratic society. In civilian programs transparency in all stages enables managers to measure public reaction before a proposal is finally adopted and implemented.

3.4 Proposals

All proposed solutions have to be weighed against goals and within the context of constraints after the problem is clearly defined. Again, in the voting example it would seem the civilian agency requires a method to verify identity of the voter. In the case of fraud, the relevant security agency requires a method to identify the perpetrator with his true name.

There are numerous alternatives to address in evaluating proposals: Is a database needed? If so, how should information be stored to best insure security and minimize privacy harm? What information is really needed? Is information on an identity card sufficient?

Evaluation of proposals and options is a complex task, taking into account constraints and considerations such as privacy, risks of data misuse, ethical considerations, public reaction and

\(^{28}\) There are exceptions, particularly with identical twins. “Monozygotic (MZ) twins are considered being genetically identical, therefore they cannot be differentiated using standard forensic DNA testing.”


\(^{29}\) There are numerous “indicative” field tests that are considered effective for investigative direction but not of a standard need for courtroom presentation.

\(^{30}\) E-mail correspondence with Lawrence Kobilinsky, Director of Forensic Science Department, John Jay College of Criminal Justice, 29 December 2014.

acceptance, system cost and reliability, implementation (training costs, data collection, data input), system maintenance (data stability), data retrieval (including false returns). This paper highlights the privacy aspects involved in biometric identification proposals and the differences between civilian and security goals.

One difference between civilian and security proposals is transparency. Civilian programs should generally be a matter of public record and discussion. Security proposals are more commonly an issue of closed door (if not officially designated “secret”) discussion.

When various solutions to the problem are recognized, presumably biometric identification would be one of them. An analysis of biometrics would include a myriad of technical issues. Should there be, for example, a chip in an identity card presented by the voter, or should there be a database? If a chip is used, should there be a backup database with the information? Part of the analysis must be system security, assessing data handling in each storage method.

Only after each proposal is evaluated according to these criteria can a tentative plan of action be chosen.

In evaluating proposals it is important to take into consideration that biometrics can pose a serious problem for proportionate identification. Limitations are in jeopardy when biometric data is incorporated into a document and swiped. One can cover information on an identity card, but one can only theoretically hide data on a chip. One is even more helpless when he is included in a database (biometric or other). That is to say, biometric data are often incorporated with other information. The same chip or other device can have both personalia (name, birth date, etc.) as well as biometrics.

### 3.4.1 Biometric Proposals

In certain cases of identity theft here is an erroneous assumption regarding the benefit of biometric files. When an imposter assumes the identity of a real person, biometrics can theoretically be used to prove fraud. That benefit, however, is more limited than commonly assumed. It applies only to the relatively few instances in which the fraud perpetrator is required to provide his biometric data. This might be appropriate during passport issuance procedures, but it does not apply, for example, to relatively wide-spread credit card fraud based upon assumed identity. That fraud is much more prevalent than voting fraud (only occurring once every few years during elections).

Biometric databases have been suggested as a method of fraud prevention. In another example a traveler’s biometric information would be stored either in a central database or a chip imbedded in the document. Major database concerns are access control, effectiveness, efficiency, cost, practicality, information security, and privacy. Major chip concerns are document loss, unauthorized information downloading, data transfer for illicit purposes, and duplication.

No system is foolproof. In one experiment regarding biometrics a lifted fingerprint was “identified” to allow access to an unauthorized person.32

Documentation raises the pragmatic issue that the need for secure documentation crosses the government / private sector line. The need for privacy, whether in biometric or traditional databases, cannot be ignored.

A database is more complex than it might at first seem. It is a collection of information that can be searched using modern computer technology. Data can be selected according to category,

---

ranging for a single person to large groups of people. Examples would be “information about John Smith” or “data concerning divorced men over 45 years of age.”

3.5 Tentative Approval

Some plans sound good on paper, but unforeseen difficulties arise when they are put into effect. For this reason approval at this stage of planning should be tentative, allowing for the chosen proposal to be approved tentatively, so that it can proceed to the next stage.

3.5.1 Selecting Biometric Identification: Justifications

It is clear that biometric data can be a definitive method of identifying an individual. There are numerous reasons why the biometric approach can be chosen. It is the purpose of this discussion to detail pro’s and con’s. The reader can draw his own conclusions. Each case must be examined on its own merits. General security is, however, one consideration that is often overlooked and should be mentioned (though not necessarily endorsed), particularly in Israel where it plays a major role.

As general background, there are biometric data users such as the military, the intelligence network, and various specialized medical-related offices. Public focus is commonly concentrated on the civilian applications of biometric databases. This is certainly natural. It must be realized, however, that biometric databases play an important role in modern intelligence work, often far from public view. There is a paradox. Civilians are frequently indignant upon learning that governments monitor personal information, yet they expect governments to succeed in thwarting terrorist activities through programs that would not be possible without some type of monitoring. Government monitoring of communications and Internet use are most often cited in intelligence operations, but biometric databases also play their part.

3.6 Testing

Many well-planned proposals do not work in reality. Hence, programs with tentative approval have to be tested. Preliminary trials can be made with fictitious data, but a larger scale test often involves true data. At that point the inter-related issues of security and privacy must be considered.

To clarify, in preliminary testing of an identification card the fictitious data of one hundred non-existent persons might be used. That constitutes a very small database. If later it is decided to use a segment of the population as a database even in a test scenario, security and privacy must be taken into consideration.

3.6.1 Security and Privacy

Security means the safekeeping of a database, so that its content cannot be accessed without authorization. Access without authorization to personalia details is an issue of privacy intrusion.

Today most of us are tracked by numerous databases. Some people are not aware that not all databases are overt or necessarily used for assumed purposes. Quite often data provide information that is used for cross-referencing and the building of marketing profiles, which the consumer eventually sees as he becomes a well-targeted object for commercial sales pitches. For

35 “The FBI and Biometric Enabled Intelligence.”
http://biometrics.org/bc2009/presentations/tuesday/DelGreco%20%20Rm14%20Tue%202000-300Pm.pdf
example, what size shoe did you buy online? Do you wear glasses? What subjects of reading material do you buy?

Read the fine print on an Internet use contract. You might be surprised as to what you see. Civilian, often commercial, use of these data is almost always allowed in the technical verbiage of a contract.

Security services have another goal. Often they are interested in the combining of all files to build a more or less complete biometric profile of a person. Biometric data gleaned from online shopping is the result of a voluntary act. Information on official documents such as an identification card is not voluntary. It is mandated by law. They combine the two.

A major threat is when official biometric data not held securely falls into unauthorized (criminal) hands, thus opening up a wide range of impersonation possibilities.

3.7 Evaluation

Is the proposed program an effective solution to the problem at hand? Does it meet all goals? Test results have to be evaluated with benchmarks (including all of the above mentioned parameters) built into the process. If the test fails, it is back to proposal discussion. If the test is a success, then the approval process can proceed. A key to the evaluation is objectivity, often ensured by outside and independent evaluators.

3.8 Implementation

Once a program has been termed to meet all requirements, it must be put into effect, a procedure that can take time. That, however, does not mean than the working committee can be disbanded. Implementation is only a marker signifying the beginning of a procedure that needs constant oversight and evaluation.

3.9 Re-evaluation

Times change. Needs change. Technology changes. A key part of every program should be periodic re-evaluation. What was appropriate yesterday will not necessarily be appropriate tomorrow.

4. Israeli Experience

The Government of Israel is confronted with numerous identification problems, but the application of the steps of conceptualization, goal definition, identification of constraints, proposal have not always been implemented fully. Government offices hold numerous databases regarding citizens. In some cases full procedures were followed in database establishment. Others were created by “shortcuts” to the system. Some databases are biometric, while others are not. For the purposes of this paper discussion is centered on two civilian (Ministry of Interior) and one security (Israel Police) biometric databases. In each case consideration is given to effectiveness, alternatives, and threats to privacy and security.

4.1 Conceptualization

Israel is faced with numerous security problems not solely typified by an opposing army wearing distinctive uniforms. In good part forces opposing Israel are individuals wearing every-day attire

37 The Israel Police has been in the Ministry of Police and the Ministry of Homeland Security (name changes) except when it was merged into the Ministry of Interior from 1977 until 1984. Police Historical Unit e-mail, 25 February 2014.
who emerge from civilian ranks, conduct adversarial acts (acts of violence supported by logistics support or intelligence gathering). Adversaries ultimately try to meld back into the civilian population. In many senses this can be deemed a tactic of anonymity, thus classic military philosophy has limited application.

4.2 Goal Definition

The goal of Israeli programs has been to find accurate means of identification given the unique challenges the country faces.

4.3 Constraints

The budget of Israeli government offices, particularly in the civilian sector, has been traditionally limited. In parallel, a lower priority has been assigned to many civilian functions. These two constraints have exerted a limiting factor on certain programs, although in recent years this trend has begun to change. Sometimes this has meant increased funding. In at least one case, a change in public opinion dictated that a weapons licensing office be transferred from a civilian to a security office.

4.4 Proposals

In selected cases Israel has taken into account experience from abroad in developing identification proposals. In recent years biometrics have played a significant role.

As the U.S. Biometrics Identity Management Agency overview states, biometrics are a key capability that can identify the enemy, denying him this anonymity he needs to hide and strike at will. In operational intelligence terms this means identifying the opposition to prevent or at least mitigate actions and their effects. For military intelligence the opposition is the confronting army or para-military force. In civilian terms today the enemy is the terrorist. The terrorist hides amongst civilians and often act like a civilian. Therefore it is only logical that the manhunt for him be amongst civilians.

Biometrics, forensic science, intelligence, and terrorism are not galaxies apart. They all meet at the terrorist incident --- in its selection, planning, and execution.

Should security and counter-terrorism be the justification for an extensive biometric database? This is not within the purview of this paper. The effectiveness of a biometric database in counter-terrorism should be mentioned and cannot be denied, but one wonders if it would be a distortion to say that such use is of importance over-riding routine civilian concerns. It is one consideration that must be weighed in the overall balance of costs, threats, and benefits, however due to classification restrictions it cannot be evaluated properly in the public sector, although after a terrorist incident public emotions run high.

Anonymity (within certain bounds) is a guarantee of democracy. It allows people to speak out without the threat of retribution or retaliation for their ideas.

The fear of civil libertarians is the possibility that certain data collection can be conducted in Israel then merged with personal biometric data collected for seemingly innocuous reasons. Could this happen? The FBI report giving an American example is frightening,

"The FBI recognizes a need to collect as much biometric data as possible within information technology systems, and to make this information accessible to all levels of law enforcement, including International agencies."\(^{39}\)

Another disturbing development comes from Bulgaria where, "Authorities set requirements that cover issuing of 25 different documents, from different types of biometric passports, over ID cards and electronic residence permit (eRP), to driver licenses and temporary documents."\(^{40}\) This means that a compatible biometric file can be built on each participating person.

The history of information leaks shows no totally secure database with multiple party access. "According to statements by the Department of Argentina Defense the computer systems area say they had a system impossible to hack, things turned otherwise." Documents classified "Secret" were hacked and leaked.\(^{41}\)

Even Canada has had database problems, "The Passport Canada website has a grave security flaw that allows easy access to the personal information (birth certificate, driver's license, dates of birth, social insurance numbers) of passport applicants."\(^{42}\)

Israel is no different from other countries. In addition to the leaking of the national identity card database, even the mayor of an Israeli city was suspected of unauthorized computer data access for illicit purposes.\(^{43}\)

Technology is advancing rapidly, and there are now non-contact methods of biometric data collection. In many cases a person will not know that his information is being put into a database. For example, an FBI report describes some of the sophisticated technology in the facial recognition initiatives. Software can distinguish between twins; 3-D facial recognition programs expand frontal, two-dimensional mug shots; and face-aging and automated face detection programs from video are available.

5. Ministry of Interior Civilian Example: Ministry of Interior & Identification Cards

The Israel Ministry of Interior is responsible for the issuance of identity cards, passports, numerous types of visas, and various types of permits and licenses.\(^{44}\) Voting stations are also run under the auspices of the Ministry of Interior. This covers a variety of problems, each involving the stages of conceptualization, clarification of goals, constraints, and proposals.

5.1. Conceptualization

There are numerous reasons why Israelis in routine situations must prove their identity and or age. This can be for employment, opening a bank account, using a credit card, voting, or even


\(^{44}\) Gun licensing was recently transferred from the Ministry of Interior to the Ministry of Public Security.
buying a bottle of beer. For these and other reasons Israel instituted a mandatory identification card for citizens.\textsuperscript{45} Over the years these documents changed from being booklets to laminated cards with a readily changeable attachment listing family relationships and residence details.

5.2. Goal Definition

One major goal is to provide documents that are not subject to fraudulent use.

Proposals are usually evaluated within the goals of (1) rendering fraudulent printing more difficult, and (2) complicating alteration by requiring the changing of data as well. The latter, of course, is applicable only in those situations in which the data and their alteration are checked. (Attempts to ascertain the true scope of the fraud problem have not yielded effective answers.)

Another source of fraudulent documentation use is lost and stolen papers. Lost / stolen licenses (no statistical differentiation is made) are problematic. Some Israeli statistics are available: 2010 – 107,582; 2011 – 93,468; 2012 – 87,919\textsuperscript{46}. No publically available government study details the disposition of these documents, other than blanket cancellation of validity. Nor are statistics available regarding privacy violations or identity theft, hence it is not possible to objectively evaluate the step from a potential danger to a real danger, and the resultant necessity of a biometric or other replacement. Hence, assessment of this phenomenon in terms of documentation goals is not as simple as it could be.

Going back to the voting example, although Israeli identification cards are commonly presented at voting polls, the officiating staff receives virtually no instruction in detecting data alterations.

Resolving the issue of voter fraud is, unfortunately, a wide-spread problem that has caused the cancellation of results in two Israeli cities following the 2013 municipal elections.\textsuperscript{47} Therefore a long term “quick fix” is inappropriate. The proposal for voter identification verification has to be tested then appropriately evaluated with benchmarks (including all of the above mentioned parameters). If the test fails, it is back to proposal discussion. If the test is a success, then the approval process can proceed.

(There are also other identity cards that are issued by various government agencies and private companies for work-clock use, personnel identification, and access authorization; some of these cards have biometric applications, but they are outside the purview of this paper.)

5.3. Constraints

One of the constraints is the bureaucratic tendency to minimalize the number of different files held by the Ministry.

Although identification cards are popularly viewed as a civilian document, in Israel they do play a certain security function. For that reason the Ministry of Interior, albeit a civilian officer, has justified the elimination of certain transparency steps in discussions about card issuance.

\textsuperscript{45} Current law is Identity Card Carrying and Displaying Act of 1982 as amended.
\textsuperscript{46} E-mail Ayyala Danino, Israel Ministry of Transportation / Freedom of Information Office, to Jay Levinson, 16 October 2013.
5.4 Proposals

As technology has advanced there have been numerous proposals to meet goals. These proposals have arisen as part of periodic re-evaluations of currently available identification technology. Several of these proposals have included the possible use of a biometric databases in one form or another in listing people (identity cards, passports) or screening applicants (visas, permits, licenses).

Although fingerprints have been known for more than one hundred years, biometrics were not as wide-spread when Israeli identity cards and passports were first issued in the early days of the State of Israel. Today, after periodic review of programs, biometrics have been supported in some circles as a method of fraud prevention.

Today Israel is faced with the governmental approval for a biometric identification program including both the implementation of biometric data and a biometric database, taking into consideration the nature and size of identification problems, cost effectiveness, and privacy concerns. Is biometric identification a cost-effective approach? Is it a desirable approach?

In Israel there are numerous types of biometric databases, some already in effect and others proposed; each is used in its own way for its own purpose, hence it is almost impossible to generalize about desirability, privacy and efficacy. Each use raises its own issues of appropriateness, cost effectiveness, security, and privacy protection. For example, the military maintains extensive biometric databases regarding soldiers for medical and victim identification purposes. The Police Rogue’s Album has a very different purpose --- the facial and posture identification of criminals.

5.4.1 Biometric Databases

For various reasons Ministry of Interior maintains numerous databases. These have been instituted after the approval stage of program development. Many have wide access, but on more than one occasion the Population Registry has failed security precautions and has been hacked. (At least two hacked versions are actually available online.) This is a prime example of the need for periodic re-evaluation of programs, not only to improve performance and to assess the meeting of changing goals, but also to enhance security and privacy.

It is the general policy of the Government of Israel that the Ministry of Interior keeps files separate from the Israel Police and other government agencies (Israel Police access to Ministry files will be discussed later), so all proposals should take this into account. This is done to insure societal and individual privacy to the greatest degree possible.

The basic implication of failed security is that extensive personal information ranging from dates and places of birth to marital status and family relationships have become a matter of open record. This hacking is just another support to the contention that even the most protected databases (such as revelations from the U.S. National Security Agency records) are potentially vulnerable.

---

48 Specified in 2009 Biometric Database Law, Section 6.
49 Access between agencies is governed by Privacy Protection Warrant (public agencies) from 1986 with revisions. The exact permissions are not included in the law. They are at the instruction of certain government officials.
It is the general policy of the Government of Israel that the Ministry of Interior keeps files separate from the Israel Police and other government agencies\(^{50}\) (Israel Police access to Ministry files will be discussed later), so all proposals should take this into account. This is done to insure societal and individual privacy to the greatest degree possible.

### 5.4.2 1982 Law

The biometric identification cards have an interesting history strewn with question and problems. Initially, the Ministry of Interior had decided to adopt biometric identification cards and passports (two fingerprints and facial scans) without a centralized database to verify bearer identification and prevent forgery. In 2007, however, the Ministry changed its policy and advocated a central database of biometric identification information. On 27 October 2008 the initiative took the form of Bill 408 presented to the Knesset as a 24 page document.

Even since the passing of the 1982 amended identification law,\(^{51}\) technology has produced changes both in document production and in document use. At one time voting in national and municipal elections could be done only after presentation of an identification booklet to prove local residence in municipal contests. Pages were stamped at the polling place with a unique cachet to prevent voting more than once. (Different elections used distinctive designs and ink to avoid confusion.)

Computerization over-rove the cachet system, and laminated cards with family details on a computer generated attachment replaced the hand-completed booklets. Check-offs on computer lists recorded who came to vote. Since 2005\(^{52}\) voting can also be done by presentation of other positive identification with a picture --- an Israeli passport or an Israeli driver’s license. In other words the role of the national identity card is slowly changing, and increasingly fewer people carry it routinely on their person.

The current theory of identification in voting and in other scenarios is based upon the photograph on the document presented, however that is problematic.\(^{53}\)\(^{54}\) Numerous incidents show errors in facial recognition that have led to mistakes --- from minor inconvenience to incarceration for a crime not committed.\(^{55}\) If eyewitness recognition testimony\(^{56}\) sometimes errs, one must realize

\(^{50}\) Access between agencies is governed by Privacy Protection Warrant (public agencies) from 1986 with revisions. The exact permissions are not included in the law. They are at the instruction of certain government officials.

\(^{51}\) Identity Card Carrying and Displaying Act of 1982

\(^{52}\) Amendment no. 54 to article no. 74 of the Election Law, approved by the Knesset on December 5, 2005.


\(^{54}\) Photo identification prior to voting in the United States is legally problematic. http://www.washingtonpost.com/blogs/govbeat/wp/2014/04/29/eight-states-have-photo-voter-id-laws-similar-to-the-one-struck-down-in-wisconsin/. Accessed 1 May 2014. Article based on United States District Court, District of Eastern Wisconsin. Case No. 11-CV-01128. Also Case No. 12-CV-00185. Decision filed 29 April 2014 is based on accessibility to photo identification and not on privacy. It is “hereby permanently enjoined from conditioning a person’s access to a ballot, either in-person or absentee, on that person’s presenting a form of photo identification. The decision contains an evaluation of voter fraud and the need for photo identification. This problem of an undue burden to produce photo identification does not exist in Israel due to different basic laws and the mandatory identification card.

\(^{55}\) For an example of a photograph mis-identification that resulted in an erroneous 23 year prison term, see http://www.innocenceproject.org/Content/Another_bad_photo_lineup_another_wrongful_conviction.php. Accessed 1 May 2014.

that photographs present additional difficulty, since they show only one perspective, lacking depth. Even with biometric identification cards it is hard to envision the biometric data on a card being examined in all situations --- maybe at a polling station prior to voting (though rather impractical given the large number of polling stations in Israel), but certainly not in a commercial, non-government situation such as a supermarket or department store. Where is the real problem that has to be solved? Voting fraud is usually relatively minimal,\(^{57}\) and a minor buying an alcoholic drink is not the core issue; the real problem is with financial transactions.

### 5.4.3 2009 Law

The 2009 Biometric Database Law\(^ {58}\) constitutes the basis for biometric data collection by the Ministry of Interior to issue identity cards. The law sets forth principles but not details.

3.a. An employee of the Ministry of Interior appointed for such purpose by the Minister is authorized to take from a resident biometric means of identification and to derive from them automatically biometric means of identification for the purpose of issuing an identification document to said resident an identification document which will include means or data as stated, ...

A reading of the law yields that conditions of the proposal are extremely vague, in this case without stipulating or specifying exactly which data are to be collected.\(^ {59}\) A database is authorized, and access is theoretically restricted, but the list of persons granted access is extensive with loopholes.

Public reaction to what became the 2009 Biometric Database Law was slow. Focus of the law was on passports and identity documents, but extended use by the Israel Police and “security agencies” was to be permitted for special purposes.\(^ {60}\) The Israeli public is accustomed to certain restrictions and conditions for security purposes, so the law raised no widespread reaction. It was only after a limited number of people sensitive to cyber phenomena raised serious objections that a relatively small segment of the public reacted.\(^ {61}\) So as a compromise a two year “voluntary pilot study” was adopted for evaluation purposes. One contention was that the two year test was designed to quell public opposition rather than conduct a serious experiment.

### 5.4. Testing

Based on the above law, in July 2013 Israel initiated a voluntary two year\(^ {62}\) pilot program to test the issuance of biometric identification cards (and passports), and their use.\(^ {63}\) Initial tests were authorized on a voluntary citizen basis in Ashdod and Rishon Le-Tziyon. Since then the program

---

\(^{57}\) Reportedly widespread fraud in the Beit Shemesh municipal elections (Jerusalem Post, 23 Oct. 2013, p. 2) is rare. It was said to include more than 200 forged identity cards. It seems that a partial and traditional solution is secret printing and a requirement to update photographs.

\(^{58}\) חוק התכנית אמצעי זיהוי ביומטריים ותוני זיהוי ביומטריים המסطرف זיהוי עם תכנית מיתר, תש"ט 2009.

\(^{59}\) For biometric information in a medical and insurance context see 1986, מנהל התفصית (בכינית צפיפ יברזים), תשנ"ג. 1986 and later amendments.

\(^{60}\) Biometric Database Law. Section 1 (2).


\(^{63}\) Most recent biometric identification law is תקנות הכללות אמצעי זיהוי ביומטריים ותוני זיהוי ביומטריים מסطرف זיהוי עם תכנית מיתר, תש"כ 2011.
was expanded with advertisements placed in wide circulation newspapers beginning 11 October 2013, inviting public participation. Internet and newspaper advertising was also initiated.

The background to the test is suspiciously vague and contradicts the principle of transparency in the evaluation of civilian-use programs. The program champion appears to be MK Meir Sheetrit, who as Minister of Interior awarded a contract to produce the cards to a company without prior competitive bidding. As chairman of a Knesset committee discussing the issuance of the cards, he expelled a photographer from a session discussing the biometric card issue.

In the two city test not all identity card applicants have opted for the biometric card. Advertisements in newspapers tried to widen the program beyond the two designated cities. Another attempt to widen the test area was to offer passports without fee to Israeli citizens opting for a biometric identification card regardless of their place of residence (even outside the test area).

In other words the Ministry of Interior moved forward to the implementation stage without waiting for the end of the testing period and full evaluation of testing results.

5.5 Evaluation

The pilot study was designed without guarantees of objective evaluation. For example, the Interior Ministry and its Population Authority designed the pilot study, were tasked with its execution, and were charged with its evaluation. There were no benchmarks and rafts specified for objective evaluation purposes. Cost versus benefits was ignored. Nor were any alternative solutions seriously studied as options to a large centralized database. No independent oversight was built into the program.

The Association for Civil Rights in Israel, weary of privacy infringements, was able to prove to the court that the “pilot study” was an invalid exercise with “built in success.”

The program had a dubious bureaucratic and legal development. On 23 July 2012 the Supreme Court declined to issue an injunction against the biometric database program, but on the other hand it cast serious doubt about both its efficacy and utility, calling into question the very necessity of a central biometric database. The Court also raised the issue of alternatives.

64 “Sheetrit ... is eager to pass this bill into law without any public debate. The bill itself allows confidential regulation and confidential procedures for use of the database and that are not subjected to any public review.” Quoted in http://972mag.com/israel-to-start-collecting-fingerprints-from-all-citizens/15686/. Accessed 12 June 2014.


As noted, the database and the design of the pilot test were deemed to be devised in such manner as to not enable true testing. The Court ruled that there must be specific criteria for success and failure. The necessity for external and independent review was also cited.68

Even though the Ministry of Interior skipped over evaluation of the proposal tested, opponents did not. Opponents contend that the wider program has not been authorized and that according to bureaucratic norm and proper practice any expansion of test cities should wait until the original authorized trial is completed and evaluated. They also note that the advertisements do not explain database dangers. This is a common complaint that has been voiced in several countries, including Great Britain and India. Once the government has decided on a program (at best after internal debate), there are attempts to sell it to lawmakers and to the public without raising negative factors.69 The issue then becomes one of the government bureaucracy against NGO’s and private individuals. As will be seen, this is what happened in Israel.

The advertising costs involved in "persuading" the public to opt for biometric cards cannot be evaluated properly, since exact budgetary figures are not available for comparison with card issuance. It can only be asked why the advertisements are necessary beyond the two test cities that have been authorized.

5.6 Public Acceptance

Public acceptance is a factor that cannot be ignored, although it can change. It can also be difficult to measure. There can be “education” programs. This is most often a gradual process of change. Events, however, can sometimes bring about an immediate change of attitude.

Although police applications of biometric databases are often outside the public purview, sometimes these databases do encounter scrutiny. The case of facial recognition is a classic example not only of public awareness, but also of suddenly changed attitudes due to external events.

To cite a foreign example, U.S. Super Bowl XXXV (2001) is a case in point. There was a public outcry when it became known that Tampa police used facial scanning to screen for criminals amongst crowds.70 Encouraging the reaction was the fact that the police found no criminals, no con artists, no bombers, and no terrorists at America’s top sports event.71 This cast doubt on the efficacy of the extremely expensive effort. Objectively seen, no criminal caught is a positive result. Facial recognition was only one part of a broad security effort that proved successful. Popular attitudes, however, are more emotional than rational. The events of 9/11 later that year rapidly changed the public mindset; the same principle of facial scanning became an accepted security method at airports. The public discussion, of course, was superficial. There was no in depth examination of database use or privacy issues.72

69 In Israel later mandated by the Supreme Court.
As part of the biometric identification card program the Ministry of Interior has initiated a one-sided campaign to encourage public acceptance.

5.7 Reevaluation and Changing Realities

A factor complicating true analysis of biometric identity card use is the growing number of drivers’ licenses in circulation, all of which today have photographs. As already noted, these are considered legal identification for virtually all purposes including voting and financial transactions, and as such they often replace national identity cards. Thus, any comprehensive biometric program would have to include driver’s licenses as a practical measure.

In putting forward identification card proposals, it seems quite apparent that there was no comprehensive survey and reevaluation of the situation on hand at the time.


There are also numerous types of Israeli travel documents designed for international travel – regular and diplomatic passports, laissez-passez, etc. Here, again, discussion is limited to regular passports issued to Israeli citizens, keeping in mind their additional use as legal for identification for purposes within the country, such as for voting.

6.1 Conceptualization

Travel documents specifying the status of the traveler (resident, citizen, diplomat, etc.) are needed to document travelers. This discussion is limited to “regular” passports issued to Israeli citizens.

6.2 Definition of Goal

As with other documents a primary goal is the production and issuance of a secure travel document difficult to use fraudulently. Lost and stolen passports pose a potential threat to that goal.

The number of lost / stolen passports is a relatively small percentage of documents issued: 2010 – 17,066 lost, 3737 reported stolen; 2011 – 17,789 lost, 3470 reported stolen; 2012 – 18,590 lost, 3628 reported stolen.73 These are not just abstract numbers. They represent the theoretical possibility of fraudulent use,74 though the working assumption is that the vast majority of “lost” documents were truly lost and not later misused. On a factual level, however, as is the case with lost and stolen driver’s licenses and identification cards, no comprehensive statistics are available regarding privacy violations and / or criminal use of these documents. Hence, the numbers provide no statistical basis in the public domain to assess the need for biometric replacement. If the public cannot accurately assess the problem, it is in a poor position to evaluate proposals to solve it.

With both identity cards and passports the government intentions are: issuance to persons using their true identity, prevention of duplicate document issuance except when known to authorities (e.g., damaged, lost or stolen documents), prevention of unauthorized alteration, and verification of authenticity. Although these are Ministry of Interior goals, the Ministry is not responsible for enforcement. A query yielded the answer that enforcement is the domain of the Israel Police\textsuperscript{75} and not the issuing authority. This also complicates subsequent proposal evaluation.

A database of lost and stolen passport numbers has been suggested. This has no direct privacy implication, but “lost” passports legitimately “found” do complicate application of such a program.

Israel is not the only country in which the phenomenon of lost and/or stolen passports poses a potential problem. Passport theft in the United Kingdom is another example that raises potential dangers for privacy. The simple reality is that passports are being stolen in increasing numbers\textsuperscript{76}. The more information a passport contains, the more information is potentially compromised. Even if “sophisticated” chips imbedded in the document “protect” the data, it still can probably be read by crime organizations with well-funded resources\textsuperscript{77}.

A summary of methods by which U.K. passports have been stolen shows the diversity of the problem: purse snatching 40%, burglary 21%, pick pocketing 13%, mugging 3%, car break-ins 16%. Although these numbers are for the U.K., statistics for other Western countries are undoubtedly similar.

6.3 Constraints

Travelers must be inspected rapidly and efficiently. This is a primary constraint in the development of any proposal.

One suggestion raised with Israel by a high ranking U.S. Customs official regards incoming trans-Atlantic passenger flights, where the dispatching country (Israel) would provide passenger and passport information upon aircraft departure from the gate. This enables checking against criminal databases and at least U.S. passport issuance records and reports of lost/stolen documents. This suggestion was made to over-ride the time constraint without giving preference to any specific proposal.

Passports must also meet the requirements of international treaties and regulations.

6.4 Proposals

Versions of biometric passports have been proposed in Israel. The focus is three-fold: exit from the country, use in foreign countries, and return to Israel. Primary security concerns have apparently focused abroad.

In terms of Israeli travel documents used abroad, there are significant problems with biometric passports, whether they are of the chip/reader or chip/database type. If the technology for

\textsuperscript{75} E-mail Mali Davidian, Ministry of Interior / Freedom of Information Office, 13 October 2013, to Jay Levinson.

reading chips is widely available, it is reasonable to believe that use of that technology is restricted to authorized government inspectors.

Advocates of proposals including databases for passport holders point out that data from illegally printed documents and stolen blank cards fraudulently issued will not be included in any database. Checking the database of issued documents is one method of fraud prevention.

On the negative side concern has been raised in proposal evaluation that foreign access to Israeli databases would have even more potential dangers.

The use of biometric passports in the Netherlands is an example of basic effectiveness. Since the enactment of the 2009 Passport Act, biometric passports have become mandatory in the Netherlands. The Act requires that two fingerprints taken in flat inoperable format appear in all newly issued passports in conjunction with the European Regulation.

From the beginning there were concerns raised to the Dutch Council of State based on the authority of the European Union to enact legislation, as well as privacy and effectiveness issues. This was in parallel to similar a case in the German courts most notably raised by Michael Schwartz, who applied for a passport in Bochem and refused to provide fingerprints; his application was denied.

Setting aside the legal arguments, the German court questioned the effectiveness of biometric passports, noting a high rate of mistakes at border control. In the Netherlands this was confirmed by the mayor of Roermond, who asserted that 21 percent of the passports issued in his city had fingerprints of a quality insufficient for identification. (This is quite similar to the Israeli experience with fingerprints taken by non-police personnel, although the exact numerical percentage of poor quality is not documented.) By April 2011 the Dutch Ministry of Interior contended that the number of false identifications (positive/negative) was too high to warrant continued use of fingerprints in biometric passports.

A common privacy complaint about biometric passports is the compilation of a citizenry database. The Dutch, however, also encountered problems with the durability of Radio Frequency Identification (RFID) chips embedded in passports and illegal reading of the fingerprints.

This Dutch experience obviously brings into serious question the reliability, hence the effectiveness, of biometric passports with clear implications for police activities. The biometric passports also do not answer the problem of genuinely issued documents based upon fraudulent supporting papers.

The security of the actual travel document is one issue. It cannot be separated, however, from passenger processing.

Use of travel documents must be divided into domestic ports of entry/exit and foreign points. In Israel international travel has dramatically increased in Ben Gurion Airport, the country’s primary port of entry/exit. This has required new methods to speed processing. Terminal 3, the main international gateway, opened on 28 October 2004. The following year slightly fewer than 9 million incoming and departing travelers were processed through border control. By 2012 that number had grown to 12.4 million. Although part of the handling solution is the construction of additional space already specified in the original plans, efficient border control of increased numbers of travelers cannot necessarily be achieved through more inspection stations and additional manpower.
Biometric passports also ignore two other possible bottlenecks in passenger processing --- security inspections upon departure and customs inspections upon arrival.

Increasing inspection space incurs not only additional manpower costs and construction issues of both finances and space. It only superficially improves the quality of inspection under the assumption that more time means better processing. True efficiency is a function of both time and accuracy, and accuracy is very much dependent upon methodology.

7. Security Example: Israel Police

In very general terms it is the objective of the Israel Police to enforce criminal law and arrest violators. The police use a wide variety of files to achieve its goals including criminal history of individuals, records of traffic violations, etc. There are also numerous biometric databases which are kept, and their secrecy implications vary. Finger and palm prints are on a national AFIS network; facial recognition (Rogue’s Album) records can also be accessed throughout the country. Handwriting (for example bogus checks) and DNA records, however, are restricted to National Headquarters laboratories.

Forensic biometric databases connect various pieces of evidence together, then the data hopefully are associated with a specific individual. For this purpose there are collections of both “raw” evidence (e.g., blood stains or hair found at the scene of a crime) and in this example the DNA of known individuals who meet certain legally specified criteria.

Unlike the example of the Ministry of Interior, the use of Police biometric files is theoretically limited to the Israel Police, and access has been increasingly controlled in recent years. Yet, access by other government agencies is permitted under certain circumstances.

The Israel Police handwriting files do not have an automated search. The bogus check file began in the pre-computerization era. It was also judged that handwriting files including the check file do not justify computerization.

The German FISH program was investigated. According to FISH operators the system contains the handwriting of PKK Turkish extremists. The system is also capable of using this and other known handwriting in the database to build writer profiles based on handwriting characteristics. Although the system was started by the Bundeskriminalamt, its use spread throughout Germany and to other countries as well. As noted, it was determined that the system was not needed in Israel.

In any event, access to all handwriting files is limited to Document Laboratory personnel.

7.1 Disaster Victim Identification (DVI) [81]

[81] Levinson, Jay; Domb, Avi. “Disaster Victim Identification In Israel : A Multi-Disciplinary Approach.” Anil Aggrawal’s Internet Journal of Forensic Medicine and Toxicology [serial online], 2013; Vol. 14, No. 2 (July –
DVI is a responsibility shared by the Israel Police and the Center for Forensic Medicine, which was once a police function, but since 1976 belongs to the Ministry of Health. In general terms the Israel Police is responsible for the collection of *ante mortem* (AM) data in the case of large incidents. The Center collects *post mortem* (PM) data. The development of the DVI program was more a case of repeated re-evaluation than pre-planning.

### 7.2 Conceptualization

The DVI program started after the 1967 Yom Kippur War as a wartime plan to identify victims of enemy attacks of the civilian population. Responsibility was given to the Israel Police, which worked under the policy auspices of the Ministry of Interior, which in turn served on a board chaired by the Ministry of Defense.

By the early 1990s this conceptualization became obsolete, but the DVI program was never formally re-evaluated. Rather, it gradually changed under the pressures of events in the field. Terrorism took a heavy toll, and the Israel Police had to react.

The Institute of Forensic Medicine had been removed from the Israel Police, so a working relationship needed to be defined. The Ministry of Interior was given a wartime-only mandate, so they did not participate in the response to terrorist acts. The Ministry of Defense also had no role. (Logistical assistance came from the IDF and not from the Ministry.)

Although the original conceptualization was no longer valid, it was replaced by Israel Police response to incidents which created a *de facto* redefinition of DVI, and not by a planned program.

There are major differences between civilian and security programs. The latter often have to make real-time changes according to developing events, even if the changes involve basic conceptualization.

### 7.3 Definition of Goal

In disaster response the goal of identification is to match the AM information of a deceased victim with the PM records of a known person. That goal remained unchanged as the program changed.

In wartime planning the Israel Police was tasked with AM and PM data collection. Response to terrorism yielded a change in responsibilities. The Israel Police is to collect AM information; the Institute of Forensic Science is tasked with PM collection. Matching depends on the type of data. For example, the Police compared fingerprints, and the Institute dealt with pathology.

To enhance coordination a police medico-forensic expert is assigned permanently to the Institute.

### 7.4 Constraints

Even given the religious and cultural priority given to rapid victim identification, visual recognition is considered insufficient for a final identification.

---

Privacy considerations prevent full searches of IDF biometric files. Records of soldiers are provided for DVI only on a name basis.

7.5 Proposals

The original DVI wartime program was put together in the Ministry of Interior by army veterans, and even after the Police took a stronger role, civilianization of thinking was a slow process.

In the first years of terrorism response there were no overall policy proposals. Changes that did occur focused on equipment, lessons learnt after debriefing, and training.

Only much later did advocates of biometric identification propose the use of central databases to determine the identification of deceased victims. Opponents pointed out that routine investigations almost always lead to AM information of the person, since people can be traced through various “leads” and missing person reports. Opponents added that investigations usually provide sufficient information, and they doubt the justification of expenditure given the infrequency of events.

This issue tends to be out of the Israeli public purview due to its technical nature and the cultural bias to rapidly identify the dead, sometimes without considering such issues as database security.

To cite two examples of victim identification and the proposed need for biometric databases, in the Swissair crash off the coast of Halifax on 2 September 1998 a piece of remains of all victims except identical twins (where DNA could not distinguish between them) was identified. Professor John Butt, at the time the Chief Pathologist of Nova Scotia, relates that the most prevalent identification method was odontology where classic police investigations secured the required AM data. In his opinion, however, today’s technology and a national DNA database would have significantly speeded identifications of Canadians and deceased citizens of other cooperating countries.

DNA has raised a different issue regarding privacy. After an air the legal next-of-kin wanted the body of the presumed relative to be identified, but he/she refused to provide DNA samples. There was reason behind the seemingly contradictory attitudes. The obvious concern was that the samples would open a Pandora’s Box of family relationships better left untouched. This is summarized by Rebecca Dresser, when she concludes, "Familial searches can also uncover mistaken beliefs about biological relatedness. Since many states lack clear rules addressing these matters, law enforcement officials can improperly discover, and disclose, important personal information about families." With a biometric database, this consideration poses a significant privacy problem. (In American law it is not clear to what extent and under what circumstances a deceased has a right to privacy, but in such a case as this the rights of living relatives should be taken into consideration.)

In the Pan Am crash in Lockerbie on 27 December 1988 the problems of identification were bureaucratic organization and vaporized (hence unrecovered) bodies. In neither of these classic

---

83 A major problem was the slow retrieval of bodies, similar to the situation after 9/11.
84 Telephone interview with Professor John Butt, 8 October 2013.
cases would the existence of a biometric database have been a decisive element, though it might have hastened the identification process.

Biometric identification is not necessarily simple. In terms of DVI, databases can provide false negatives.⁸⁶ Damage to the face or physical *post mortem* changes can effect identification. There have also been cases of comparing wrong fingers.

### 7.6 Re-evaluation

As of this writing there has been no organized re-evaluation on DVI on an inter-agency basis and serious discussion of an overall proposal.

In the bureaucratic context it is also hard to test and evaluate a DVI proposal. A true test can come only after a full scale incident, which obviously no one wants.

### 8. Conclusions

<table>
<thead>
<tr>
<th>Stage</th>
<th>Civilian</th>
<th>Security</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conceptualization</td>
<td>Necessary</td>
<td>Often overridden by developing events</td>
<td></td>
</tr>
<tr>
<td>Goals</td>
<td>Necessary</td>
<td>Necessary</td>
<td>Often change</td>
</tr>
<tr>
<td>Constraints</td>
<td>Necessary to be taken into consideration</td>
<td>Present, but sometimes ignored in the name of expediency</td>
<td>In at least one case expediency dictated biometric DVI data transfer outside authorized channel</td>
</tr>
<tr>
<td>Proposals</td>
<td>Necessary. Public disclosure and discussion.</td>
<td>Necessary. Often no public disclosure or vague legal authorization</td>
<td></td>
</tr>
<tr>
<td>Re-evaluation</td>
<td>Necessary</td>
<td>Necessary</td>
<td>Independent resource should be involved</td>
</tr>
</tbody>
</table>

There are differences in the reasons biometric databases are built in the civilian and security government offices. These differences are expressed in purpose and in the relative costs of data acquisition, storage, and retrieval. Although civilian and security databases are theoretically kept separate in Israel. There are laws that allow data sharing. Thus, under certain circumstances (legal or otherwise) the possibility exists of building extensive files about individuals.

The right to privacy is recognized in enacted laws, but protection against infringement is not hermetic. A blatant example is the unauthorized availability of the Citizen’s Registry on the Internet. The Israel Ministry of Interior has started a trial program of biometric identification cards. Many aspects of the program are unclear, including data management, collection necessity, and privacy guarantees.

It is impossible in the public sector to evaluate cost effectiveness of proposed biometric identification cards in Israel, since access to sufficient data is restricted.

---

⁸⁶ For false matches and non-matches in the proposed biometric program see Knesset law 7197, 27 December 2012.
A more open evaluation of governmental biometric databases in general and identification cards in specific is certainly in order. Need, cost, and privacy must be part of that public discussion before any further programs are advanced.