Prepared Remarks of
Richard Haddock, President
Drexler Technology Corporation
before the
United States Senate Judiciary Committee
Subcommittee on Technology, Terrorism, and Government Information
November 14, 2001
"Biometric Identifiers and the Modern Face of Terror:
New Technologies in the Global War on Terrorism"
[available at
http://www.iwar.org.uk/comsec/resources/senate-biometrics/te111401st-haddock.htm]

Mr. Chairman, distinguished members of the Senate Subcommittee on Technology, Terrorism, and Government Information, my fellow panelists:

Thank you for the opportunity to share my professional opinion with you regarding the application of biometric identifiers in our global war on terrorism.

My name is Richard Haddock. I am President and Chief Operating Officer of Drexler Technology Corporation a public company located in Mountain View, California, and traded on the NASDAQ as DRXR. We market our optical memory card products through our subsidiary, LaserCard Systems Corporation.

I have personally been involved with the invention and commercialization of highly secure optical memory cards for more than 20 years. These unique cards - called LASERCARDS® - have come to be known as the "world's most counterfeit resistant" identification cards. This technology was invented here in the United States by Drexler Technology, an American company. Drexler manufactures optical cards and systems for sale worldwide from our facilities in Silicon Valley.

I am here today because my company has extensive experience utilizing various biometric technologies as part of the unique security design of an optical card identification system. Each of the technologies discussed by my fellow panel members could be and, in some cases, already are being used in secure optical memory card identification systems. In fact, ALL of the technologies described here today, plus others currently available, could be combined on one card to facilitate various levels of secure authorization and multiple site interfaces

without the need for a central database of personal information or required on-line access everywhere identification is needed.

I would like to organize my remarks into three parts --

1. How to best use biometric identifiers for personal identification;
2. What a secure identification card is;
3. Field experience with biometrics on secure ID cards

How to Best Use Biometric Identifiers for Personal Identification.

It is important at this point to recognize that I am a technologist and not someone who makes public policy. However, as an American, I can also see both sides of the long-standing debate over personal privacy as it relates to recent discussions in the press about national databases and even a national ID card.

I enjoy my personal freedoms but I am also greatly disturbed by the ease with which innocent people can be horribly impacted by persons having criminal intent - whether it be by gaining unauthorized access to our Nation and its services or by simply stealing one person's identity.

This must stop. And, we have the technology to do so today.

From my perspective in the Silicon Valley, it seems that the primary focus of the current national identification debate is (1) whether or not we need a national database containing each citizen's personal information; and (2) whether the American public would feel comfortable having to show an identification card to receive services.

From my perspective, there is no question that there needs to be some form of national database or, at the very least, a sharing of information between key databases to ensure that threats are identified and cannot hide. Without such information, how could we ever expect to issue valid personal identification of any type?

The issuance of personal identification, such as drivers licenses, must be based upon an assurance that the persons being provided such documents are who they say they are and, further, that they are qualified to receive specific services and are not perceived to be a threat to those services or for any other services for which the personal identification might be used. The only way to do this is to check their applications against databases deemed appropriate by the issuing

authority and positively identify them each time they request controlled services, such as air transportation. However, those databases do not need and should not contain personal information about our citizens.

The requirement that I show personal identification to receive services has never concerned me, nor does it appear to concern the majority of Americans.

In addition, I must have shown my drivers license at least a dozen times just getting here to meet with you today. It seems that everyone wants to see a "photo ID" these days. Unfortunately, I would be very surprised if anyone who inspected my drivers license could really tell if it was a valid ID and that I am really who I say I am.

That's where biometric identifiers come in.

As you might expect, my primary concern is the security of the personal identification document, itself - how certain can we be that the document is valid and that the person presenting it is in fact the person authorized by it? This is true whether the document is a passport, visa, pilot's license, drivers license, or frequent flyer card.

We can no longer permit any identification document, like a drivers license, to be used for higher level authorizations, like airline passenger check-in, without first considering the security level of the issuance criteria and the security of the document, itself.

It is this fundamental fact that tends to lead us all into the debate about central databases and national identification. In my opinion, such a debate is not necessary.

One central identification database or on-line identification card will not solve our Nation's security problem - it is far too complex an issue. Such a solution would merely create more problems by requiring that extraordinary amounts of personal information must be kept in central databases for even the most basic level of service request.

Even beyond privacy concerns is the technical reality that highly centralized, on-line systems are subject to overload, system-related failures, hacking, and cyber-terrorism. Creating a central database, national identification system that is always online could provide a single point of failure for our entire society if our enemies ever targeted it.

What a Secure Identification Card Is.

No matter whether it is a drivers license or frequent flyer card, a secure identification card is a personal identification document, which verifies that a person is who he says he is, is not a threat, and has authorization for the requested service or activity.

As I have said, authorization for the requested service or activity must be determined at application and re-validated periodically during the life of that authorization. This requires some form of national database screening at a level consistent with the security needs of the authorization. Such checking can also be used to verify that the person is not a potential threat.

Verifying that the person is really who he says he is requires three things: (1) a secure identification card that cannot be easily counterfeited; (3) a biometric means to link the person to that card with certainty; and (3) a secure automated interface to verify that the person and card links are valid.

To avoid privacy concerns, the databases used during application should only be those determined to be relevant to the requested services. All other personal data, including biometric identifiers, should be retained by the individual on his or her secure identification card.

How would this work?

When an individual requests specific services or benefits (for example, an airline frequent flyer card to minimize check-in delays), an application would be submitted, reviewed, and approved. Next, a secure card would be issued containing multiple biometric identifiers, which can be read and verified by automatic readers at access or authorization points.

When the cardholder requests specific services (such as e-ticket check-in at an airport kiosk), the cardholder's identity can be quickly run against an on-line threat database without any personal information being transmitted from the card. Moving through screening stations, such as carry-on inspection and gate check-in at an airport, can be accomplished with off-line access control readers. The cardholder would be matched against a selected biometric or combination of biometrics found on his or her card (such as a fingerprint, iris scan, face, hand, or finger geometry). The time required to make such a match, linking the cardholder to the card, is less than 5 seconds.

Please note that I suggested a "selected biometric or combination of biometrics" in this brief scenario.

Biometric identifiers are not perfect. Each has a margin for error. To avoid rejection as well as the possibility that someone might try to defeat a one-biometric system, multiple biometric identifiers are highly recommended.

We have also found that not all locations will necessarily want to use the same method of biometric identification. In fact, our experience indicates that there is considerable interest in using a random combination of biometrics so that the cardholder will not know what biometric is being evaluated at any given time. This is definitely possible with current technology.

Field Experiences With Biometrics and Secure ID Cards

The product we manufacture, the LaserCard optical memory card, has the highest memory capacity of in standard ISO credit card format. This capacity is about 200 - 500 times more than the highest smart "IC: cards on the market today. More importantly, we have had this high capacity card in the market for more than a decade, which has allowed our users to implement any and all biometric solutions offered in the market for many years, including all you have hear about here today.

It is due to the optical cards ability to store multiple biometric files and templates that almost all industry biometric devices have been linked into optical cards, and in most cases, more than one type of biometric data has been stored. The permanent, non-erasable laser recorded media makes optical cards are the natural vehicle for secure, biometric based ID cards.

Examples of these applications include, most significantly, the US Immigration and Naturalization Service's Permanent Resident Card (the "Green Card"), which contains about 80,000 bytes of biometric information, biometric files are stored in an INS secure partition on the card, accessible only through the use of INS controlled secure field readers. Included in this data zone are:

" high quality color image of the card holder (as printed on the card surface)
" FBI quality gray scale fingerprint image of the card holder
" Digitized image of the card holders signature

Additionally, the US Department of States' "LaserVisa" border crossing card for Mexican citizens entering the U.S. has the same technology used on it, but adds even more biometric information to the card by the addition of two fingerprint minutiae files on the card to supplement the full image files stored.

Together, with more than 10 million of such cards in circulation within the US today, these cards represent the largest high security, biometrics based, ID card program in US history. It is estimated that by the end of next year, this total will rise to 20 million cardholders.

Many smaller programs have been launched since using optical cards and biometrics in the past ten years, and these programs give a good insight into what is necessary to achieve a secure and cost effective ID card system.

We have teamed with Unisys to design a border entry system using both Iris Scan and Digital Persona fingerprint systems.

We have worked in Hong Kong on the implementation of a pilot immigration control system there using both Identix fingerprint scanners and Recognition Systems Hand Geometry Systems.

We have implemented Identix fingerprint scanners for a banking card in the Czech Republic, and have supplied hand geometry systems to our resellers worldwide.

We have implemented signature verification systems using Checkmate systems, and those from CIC. Our cards have been used with voice recognition and face recognition, as well as two finger "Digi-Two" finger geometry biometric systems.

In short, we believe that we have the most extensive biometric based experience of any card supplier, since we always had the ability to store and implements any and all biometrics from a single card. No database connection is required for our totally off-line verification system approach to these biometric systems.

Based on this long-term experience with all forms of biometric devices, we have developed our own view of the best approach to a biometric ID system. The key elements of such a system are:

" Implement more than one type of biometric
" Allow room to add new biometrics seamlessly
" Assure off-line verification ability

" Provide for selection of appropriate biometric based on application requirements
" Assure integrity of the biometric files from issuer to user

Explaining in more detail:

Implement more than one type of biometric: There is no perfect biometric system. All systems have their strengths and weaknesses, and vulnerabilities. The selection of a single biometric for any large-scale system invites a concerted effort to defeat any given biometric, which will be done. This was the experience in the Hong Kong pilot, where both fingerprint and hand geometry systems were targeted by the test system, and both were shown to have vulnerabilities. The same is true for Iris scan and face recognition systems. Examples of failure modes include false fingertips; rubber hand molds, glass eyes, contact lens, and actors face make-up techniques.

Adding to the complexity is the need to accommodate the disabled and handicapped in any public access system. Considerations include:

" IrisScan system needs to accommodate the height ranges from children, wheelchairs, and basketball players, blind eye without eyes or glass eyes
" Hand Geometry system needs to work in hand size ranges from small children and Asian women's' hands through football players, plus the fact that not all people have right hands. Sanitation concerns must be addressed as well, given concern over germs and disease.
" Fingerprint systems need to address the same sanitation concerns as Hand Geometry, plus the ease of false fingertips and other substitution methods. Proprietary template algorithms and changing standards need to be addressed as well. The fact that many older people and some from the manual labor ranks have essentially non-existent or non-usable fingerprints needs to be accommodated as well. The inclusion of all ten fingerprint files and templates onto the card would help to eliminate this problem
" Face recognition will not be acceptable to many in the Moslem religion, is subject to many ACLU concerns. A best "one-to-one" match of the highest reliability requires several views to be stored, increasing template file sixes to the range of 30,000 bytes. While this is no problem when stored on an optical memory card, it is beyond the range of any other ID card to deal with.
" Signature, voice, fingers, retina, and other biometrics all have similar weaknesses

In summary, it is our opinion that more than one biometric be implemented on any secure ID card system, and that the selection of the biometric to be used by

any given application at any given time not be known to the cardholder in advance.

This "redundant and random" biometric approach will greatly enhance the overall system security, reduce single vendor dependence, and allow the tailoring the system to accommodate all citizens, regardless of their race, religion, age, handicap status, or other limitations relative to a given biometric approach.

It is for the above reasons we recommend the use of two or more biometric elements in any secure ID card system.

Allow room to add new biometrics seamlessly: Any ID card system storing biometrics in a secure form will have a significant card issuing cost, which means card life and updatability is important. The INS and Department of State optical cards have a ten-year expiration period, more than five years beyond any smart "IC" card warranty. This is a long time, and technology will change. The card should be capable of being updated and upgraded in this period, as new biometrics, software, and application requirements come along. This means one of two things: either your have an erasable, changeable media like a ":smart "IC" chip card - and live with the risk of an changeable and erasable media, or use a media having enough update media, such as the optical card, which is permanent recording media, with an audit trail to the previous information. This was a key feature for both the INS and the State Department in the selection of the optical card, since it allows them to update the card without the need to re-issue it.

ASSURE OFF-LINE VERIFICATION ABILITY: Any ID card system should be capable of complete, secure verification of the cardholder to the card without any dependence on a on-line database, although it may be present. The failure of many online systems to date to be effective, including the INS "INSPASS" program, is the total dependence on a nationwide 100% uptime, on-line database to verify the cardholder ID and allow entry. Most INSPASS system downtime to due to network and communication failures, and has constricted the system implementation to less than 100,000 people across the many years the program has been in place. Having the ability to completely verify the cardholder to the card off-line, using local black-lists in each terminal, would eliminate this problem. Additionally, the off-line capability allows the implementation of mobile and hand held reader terminal, which can greatly expand the value and usefulness of any ID card system.

Provide for selection of appropriate biometric based on application requirements: Having multiple biometrics on one card means you have the ability to select the

most appropriate type for a given situation or application. Using Hand Geometry on doors, face recognition in terminal access points, Iris scan at high security zones, and fingerprints for ticket check in, could all be accomplished seamlessly with one card, optimizing each technology for a given area. The added benefit of this is the use of multiple biometrics throughout a given system greatly enhances the overall system secure, since breaching one biometric does not cause a total system failure. If such a breach is recognized, then system applications could easily be re-programmed to select another card biometric, without the need to re-issue cards. Given the growth of technology and biometrics in general, this is a very important consideration of any new system design.

Assure integrity of the biometric files from issuer to user: In any system design using biometric for ID, it is essential to ensure that the biometric file added to the card at the time of issuance cannot be tampered with, erased, or substituted. Without such safeguards in place, there is no security, since anyone can obtain a similar biometric system, create their own biometric template files, and substitute them into the valid ID card. All card systems attempt to minimize this risk, however, only the non-erasable optical memory card can intrinsically eliminate this concern, because the laser writing process, like punching holes in paper, is physically impossible to erase or overwrite.

All Smart "IC" chip cards hold such critical information in their "EEPROM" memory; meaning "Electrically Erasable Programmable Read Only Memory", which means no such assurance can be had.

No other card data storage technology, from barcodes to magnetic stripes, is appropriate for secure biometric information that must be updated, yet secure.

Summary: In closing, I would like to point out that the INS and Department of State LaserVisa secure ID cards represent the most advanced biometric card systems in the US, and perhaps the world. The cards have a minimum of three biometric files each, and are vendor independent in their ability to be verified. The cards storage of up to 80,000 bytes of biometric data is ten times more biometric information than available on any other type of ID card, and yet uses less than 20% of the available card memory.

Other governments are following the lead of the INS: The Italian government has started issuing optical memory based ID cards as the basis of their new National ID card, and tenders from many other countries are specifying the use of optical memory to base their biometrically secured ID card systems.

Use biometrics for any ID card system, and for full security, flexibility, and long-term system life, the use more than one biometric on the card is highly recommended.

I will be pleased to answer any questions you may have.

QUESTIONS

The following list of questions expands upon key points made in my prepared remarks:

1. It appears that you prefer off-line systems to on-line systems. Why?

There are several reasons. The primary reason is that, like most Americans, I am extremely uncomfortable knowing that my personal information, including my signature, photo, voice, fingerprint, etc., might be stored on some huge government database and I would have no control over who might access these data and for what purposes. My next biggest concern is cyber-terrorism. Central databases simply become ripe targets for anyone having ill intent. Then there are the practical considerations of database design which involve access time, data transfer time, etc. I feel most comfortable recommending a solution that makes it possible for the individual to control personal data and in which the secure card interface can be used either on-line or off-line.

2. You say that the smart card has limited capability to handle biometric templates when compared with your card technology. What do you mean?

The memory capacity of a smart card is typically around 8Kbytes whereas the optical card is more than 4 Mbytes (500 times larger). The Visionics face recognition engine that we are currently using averages 30Kbytes for a 1-to-1 verification template. There is also the question as to whether the issuer wants to use only the "biometric template" or the full "biometric image." The difference is, very simply, accuracy. Although larger smart card memories are available, they are still only in the range of 32-64Kbytes at this point. The smart card simply does not have sufficient available memory for multiple biometrics plus any additional data that might be desired by the issuer.

3. What is the advantage of having updateable but non-alterable data on the optical card?

Data can be written to the card at any time but it can never be erased or changed. Therefore, the need for complicated encryption schemes and special keys to protect data on a smart card does not exist with the optical card.

4. What could make the INS and Department of State card programs more of a success from your point of view?

The INS Permanent Resident Card ("Green Card") and U.S. Department of State Border Crosser Card ("LaserVisa") are the most secure ID cards now in use in the United States. These cards have effectively eliminated counterfeiting, which was

a major problem before the INS issued the first optical cards in 1997. However, neither of these programs has fully realized their true potential because the biometric features have never been used in automatic card readers.