



Biometrics & Personally Identifiable Information:

**Assessing the Impact of U.S. Policy and Laws on the Use
of Biometrics by Government Agencies**

and

**Evaluating Solutions to Meet Government Operational
Requirements**

Biometrics in National Security

2010

Table of Contents

Executive Summary.....4

Background and Basis.....5

U.S. Government Laws and Policy: Personally Identifiable Information.....6

 The Privacy Act of 1974.....6

 Federal Information Security and Management Act of 2002.....7

Executive Office of the President.....8

 Office of Management and Budget.....9

 National Science & Technology Council.....9

 The General Accounting Office Report.....11

 Homeland Security Presidential Directive 24.....10

Impact on Government Operations.....12

 Department of Defense.....13

 Department of Homeland Security.....15

 Department of Justice.....17

 Department of State.....18

 Other Agencies.....18

Current Status.....19

 Biometrics as PII.....19

 Defining the Mission and Purpose of Biometrics Datasets.....19

Solutions.....20

 Commercial Off-the-Shelf Products.....20

 PerSay.....20

 Biometric Based Hash Codes, priv-ID.....21

Emerging and Developing Technologies.....22

 Anonymous Recognition.....22

 Revocable Biotokens.....23

Conclusions.....25

 In Summary.....27

 Appendix "A" - Interview with PerSay Inc.....

Appendix "B" - Interview with Priv-ID.....35

Appendix "C" - Interview with Securics Inc.....43

Appendix "D" -Matrix of Privacy Enhancing Technologies (PET's).....58

Executive Summary

Federal requirements to safeguard sensitive personal information date to the Privacy Act of 1974. Since then government agencies have been required to document systems of records that contain data that, if disclosed, could violate the terms of that act and potentially bring harm to people whose information is stored in those systems. Only within the past decade, however, have questions been raised as to whether biometric data -- usually in the form of encrypted templates of a person's face, iris, voice, vein pattern, hand, fingerprint, etc. -- is protected under the Privacy Act and succeeding legislation such as the Federal Information Security and Management Act of 2002 (FISMA).

As this debate worked its way through the policymaking process, new security initiatives were being mandated in the aftermath of September 11. One presidential directive specifies that all government employees and contractors were to be identified through the use of biometrics that could be shared between departments of the Executive Branch; another requires agencies to share biometric information on those who may pose a risk to national security. With these competing imperatives to both protect and share information, both the Government Accountability Office (GAO) and the Office of Management and Budget (OMB) agreed that biometrics were Personally Identifiable Information (PII) and thus subject to protection.

With this framework setting the stage, the report first looks at measures taken to ensure agencies comply with data protection requirements as they relate to biometrics. Next, it reviews the steps government officials have taken to comply with both sharing and safeguarding requirements. Finally, the document examines technologies that have been developed to overcome operational impediments that arise from having to meet both criteria.

Interviews with government managers found that agencies have incorporated extensive -- and often labor intensive -- review processes to guarantee that biometric information is used and exchanged properly. Privacy experts have become an inherent part of the development process, training has enabled workers to identify how data can and cannot be used, and the adoption of review boards to scrutinize an agency's application of PII guidance. Most of these steps relate to the directive covering the sharing of biometrics to improve national security.

Less progress has been made in implementing a truly interchangeable system of identification for government employees and contract staff. Government-wide requirements for creating and issuing identification cards have been clearly defined, but settling on a common architecture, enabling the means to vet the identity of over seventeen million affected workers, and instituting biometric-based identity checks at the door remain among the challenges yet to be fully addressed. This circumstance is partially due to the immense coordination effort required to achieve such a level of harmonization, and also because there have been questions about the ability to effectively implement an ambitious plan without risking unauthorized disclosure of PII.

Research into the technologies that are either on the market or soon to be available revealed that solutions exist that have the potential to expedite the deployment of large scale identity management

systems without threatening the security of the data. One approach makes a registrant's biometric information anonymous in such a way as to enable identity to be confirmed across agency, sector, and international lines without compromise; two others facilitate biometric identification in the field without having to exchange an actual biometric template over unsecure networks; and yet another demonstrates how identity can be confirmed via phone networks without special equipment.

Government managers who are faced with developing and implementing these complex systems will find that there are technologies that can help overcome some of the most problematic operational and legal hurdles. Whether used singly or in combination, these solutions offer the potential to expand the reach and utility of biometrics in enforcement, anti-terrorism, and identity management programs without risking disclosure.

Background and Basis

The National Biometric Security Project (NBSP) is a nonprofit organization under contract to the National Security Agency. For Fiscal Year 2010 NBSP has been tasked with researching and evaluating the impact of government laws and policy as they relate to the use of biometrics by Federal agencies. Of specific interest is a January 2008 report by the GAO that includes biometrics in the definition of PII, and a May 2007 requirement from the OMB that does the same. Under a presidential directive issued in June 2008, all Federal executive departments are required to follow common procedures for the collection and storage of biometric data, making the GAO report and the OMB instructions the de facto framework for the conditions under which such procedures are adopted and operational programs are conducted.

In reaching its conclusion on the linkage between biometrics and PII, GAO cited several precedents, the first of which is the Privacy Act. Under this statute Federal agencies were, for the first time, made legally responsible for the protection of personal information. Second, under FISMA agencies were required to implement comprehensive programs to ensure that information systems housing personal data were secure. The OMB subsequently issued technical guidance on methods to protect against unauthorized disclosure of PII, including encryption, oversight and reporting of breaches to people who may have been affected by a disclosure.

The Privacy Act legislation preceded the widespread use of biometrics by many years. In the early 1970s, biometric technology was in its infancy and largely confined to criminal identification programs conducted by the Federal Bureau of Investigation. By 2002, applications of biometric technology were in widespread use in both commercial and government sectors yet, while FISMA articulated requirements for protecting PII, the law did not further define which data elements – biometric information or otherwise – were to be covered by the law. The GAO report and OMB directive effectively closed this gap, with both documents stating in a footnote that biometrics were on a level with name, Social Security number (SSN) and date of birth as information that could be used to trace an individual's identity.

GAO authors confirmed that the 2007 OMB directive served as the source for their definition. Concurrently, the National Science and Technology Council, the science policy organization within the Executive Office of the President, indicates with absolute clarity and thoroughness that biometrics must be regarded as personal information when considering what steps must be taken to protect privacy.

Of relevance to this task, however, the NSTC also notes that biometrics provide an opportunity to *protect* privacy while connecting information and individuals in a "reliable and respectful" way. The basis for this assertion lies in the nature of the technology, which relies on algorithms to create templates that represent biometric images. Such templates, standing on their own, do not reveal personal information until they are associated with other data about an individual. The challenge faced by government agencies is to determine the right combination of technical solutions, policies and implementation practices that maintain an effective barrier between biometrics and other forms of PII, yet enable the use of biometrics in critical programs to prevent terrorism, identify criminals, safeguard the warfighter, protect government facilities, and provide innovative services to the public.

This report documents the body of government privacy laws and policies that affect the use of biometrics, describes the issues faced by government managers and executives in implementing programs as a result of classifying biometrics as PII, and details some of the solutions that may give government agencies the means to resolve those problems.

U.S. Government Laws and Policy: Personally Identifiable Information

The Privacy Act of 1974

The United States was one of the first countries to react to concerns about how computerized databases could affect privacy rights. This legislation resulted from a recommendation by the Department of Health, Education and Welfare (HEW) that a law was needed to institutionalize what it called a Code of Fair Information Practices. The Code consisted of the following principles:

- The existence of any record-keeping systems should not be kept secret
- Individuals must have a way of finding out what information is being held and how it is used
- Individuals must be able to prevent information from being collected for one purpose and used for another
- Individuals should be able to correct or amend information that is being held
- Organizations must assure the data is reliable and take precautions to prevent its misuse

In a significant step that recognized the importance of key identifiers for individuals, HEW also recommended that restrictions be placed on the collection and housing of SSNs. In doing so, HEW noted that it would serve as a means of creating a "standard universal identifier" since it could be used as a

link to all records held by all agencies. To curb abuse, HEW suggested that an SSN should not be required unless specifically authorized by Congress.

To a large extent the HEW recommendations were adopted by Congress, the result being the enactment of a law that established controls on PII and placed the onus on government to monitor the use of data and comply with extensive reporting requirements. Although certain agencies were excluded from coverage, most Federal executive departments and all state and local governments¹ were subject to restrictions on the collection of SSNs. In addition the new statute imposed broad administrative requirements on U.S. government agencies. These included:

- Requiring the issuance of a public notice in the Federal Register detailing any "system of records" maintained by the agency
- Providing access to records, allowing the individual to review and make copies of records
- Limiting disclosure to specific circumstances authorized by the law, including information released in connection with routine internal use, a census, a compelling need relating to health or safety, a court order, civil or criminal legal proceedings, and to Congress

The law also specified that an agency must limit data collection to that which is "relevant and necessary" to accomplish its purpose, and is prohibited from doing interagency matching of records unless done under the conditions of an agreement that is subject to review by Congress. Also, criminal and civil penalties are prescribed for violations. Any nexus between the Privacy Act and the collection of biometrics was unclear for nearly thirty years after Congress imposed limits on data collection, storage and management. Were biometrics true identifiers? The technical explanation may have been a qualified "no" -- unlike SSNs, biometrics, at least in template form, were and remain virtually impossible to reverse engineer or crack by brute force,² and therefore serve as a useful tool in stealing or falsifying an identity.

As the use of biometrics in the form of systems to track terrorists or streamline identity verification at federal facilities grew during the first decade of the 21st Century, a policy shift was occurring. This shift would lead to ranking biometric features, regardless of how they were collected or in what form they were housed, on par with SSNs and other data elements that could be used to commit fraud or penetrate security.

Federal Information Security and Management Act of 2002

While the Privacy Act made it clear that government-held "systems of records" must be subject to scrutiny and, with limited exception, access, legislation on how to secure those records was not forthcoming until passage of FISMA nearly thirty years later. Under the provisions of FISMA, agencies

¹ Since the SSN is issued by the Federal Government, Section 7 of the Privacy Act places restrictions on the use of the SSN that also are applicable to state and local governments.

² *Encyclopedia of Biometrics*, Stan Z. Li and Anil K. Jain, Springer, 2009, New York, NY

were mandated to address cybersecurity threats and secure PII within information systems at all levels, including within portable devices.

The driving force behind enactment of FISMA was the recognition that information security was vital to the national security and economic interests of the U.S., and that legislation was needed to provide a "comprehensive framework" for ensuring the effectiveness of controls over systems used to support the operations and assets of the Federal Government. To accomplish this, FISMA specified that agencies must comply with seven requirements:

1. Develop and maintain an inventory of information systems operated or controlled by the agency
2. Categorize information and information systems according to security risk levels
3. Ensure that systems meet minimum security requirements
4. Identify potential threats, map controls to specific vulnerabilities, and calculate the impact of the vulnerability if systems are penetrated
5. Develop a policy for the system security planning process
6. To make the process accountable, have a senior agency official certify that the controls are functioning properly
7. Monitor security on a continuous basis, ensuring that controls are updated as components and configurations change

As a result of FISMA and the companion e-Government Act of 2002, new processes were put in place³ that required agencies to evaluate the impact on privacy in conjunction with systems risk assessments. Without taking into account the privacy enhancing features of biometrics, these instructions stipulated that any government database containing biometric information was subject to a review that treated such data as that which could undermine the economic interests of the country. Under the assumption that the compromise of biometric data could further exacerbate an identity theft problem that was estimated to be \$46 billion in 2006, biometrics suddenly rose to the top of the list of data elements that could damage the economy if compromised by intrusion or inadvertent release.

Executive Office of the President

As of mid-2006, biometric information had yet to be identified as PII in any action by Congress or formal policy instruction from the Executive Branch. As noted above, privacy impact reports prepared under the provisions of FISMA often listed biometrics as a potential risk factor and raised awareness of the technology as an element that might be exploited by those seeking to steal identities, cripple law enforcement systems or weaken counterterrorism efforts. Whether by coincidence or design, that gap was closed in the autumn of 2006 with the release of two key documents within four days of each other that September. One formally advised executive agencies how to respond to a breach that resulted in

³ Per OMB guidance in May 2006 and September 2007; see "Office of Management and Budget" below

the disclosure of PII; the second closely linked biometrics with privacy and offered insights into the linkage between privacy and the control of biometric information.

Office of Management and Budget

In May 2006 Executive Order 13402 established the President's Identity Theft Task Force. Although the full results of the its efforts were not published until 2007, the lack of a cohesive means of reporting data breaches by executive agencies led the group to issue early guidance on how to handle such intrusions. The unnumbered memorandum dated September 20, 2006, issued under the authority of the Office of Management and Budget (OMB) and distributed to all departments, instructed agencies to take three immediate steps:

1. Identify a core response group that can be convened in the event of a breach
2. Task the response group with performing a risk analysis to determine if an incident has caused problems related to identity theft
3. Respond publicly to the breach with a risk-based approach that is tailored to the circumstances

In the course of describing the types of incidents that may create a problem, the task force noted that the release of a name in a report would raise little risk, but that "an SSN standing alone can generate identity theft." The memorandum further states that "combinations of information" can have the same result as the release of an SSN, stating that a name, address, or telephone number can generate identity theft when accompanied by *any one* of several other data elements, including a government issued identification number (e.g., driver's license), *a biometric record*, a financial account number with a PIN, *or any other factor that could link a profile to a specific individual.* This OMB-endorsed instruction had the effect of ending any debate about whether or not a biometric record in any form was or was not personally identifiable information. The memorandum made no attempt to distinguish between a photograph or a facial recognition template, or the relationship between a biometric and a system in which it would have to be used to be of any value to an identity thief. These omissions aside, biometrics were now equated with the most sensitive of personal data for purposes of protecting systems and responding to security breaches.⁴

Less than a year later, OMB followed up the task force memorandum with an unambiguous requirement. Memorandum M-07-16 dated May 22, 2007, instructed Federal agencies to implement a breach notification policy with 120 days. The memo cited Identity Theft Task Force findings as the basis for mandatory actions to be taken throughout the Executive Branch. In defining PII, the document placed biometrics on par with name and SSN as data that, standing alone, was considered to be personally identifiable information. While the NSTC was not willing to go that far in its deliberations about the relationship between biometrics and privacy (see below), OMB instructions left no doubt about the sensitivity of biometric databases no matter how compartmentalized that information is.

⁴ OMB Memorandum "Recommendations for Identity Theft Related Data Breach Notification," September 2006; see: http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2006/task_force_theft_memo.pdf

National Science & Technology Council

Whether by coincidence or intent, the NSTC issued a lengthy discussion of privacy and biometrics in its report, "Privacy & Biometrics: Building a Conceptual Foundation" just four days before OMB distributed the initial guidance from the Identity Theft Task Force in 2006. This primer on the technology and the relationship of biometrics to preserving privacy contains a warning that data that may not appear to be personal information could become personal information through use. Echoing the language of the task force memorandum, the report also cautions that "if data that does not directly identify an individual is used in combination with other data that also does not directly identify an individual, and if the resulting combined data could be used to identify an individual...then the data becomes personal information and privacy issues may exist..."

Leaving no room for interpretation, the report further elaborates on the nexus between biometrics and personal data:

"As a general matter, where there is biometric information there is personal information... Even though a biometric system may contain biometric data that cannot be guaranteed to identify a specific individual, the nature of biometric data...is still covered by the definition of "personal information..."

Importantly, the NSTC report also notes the value of using biometric systems to protect privacy; in fact, the report concludes by pointing out that an ongoing dialog should ensure that the evolution of privacy policy and biometric technology "advance in harmony rather than in isolation." Nevertheless, the publication of such a clear pronouncement left no doubt that senior government policymakers would henceforth regard biometrics as synonymous with PII.

Homeland Security Presidential Directive 24

Orders from the Office of the President to improve homeland security were initiated in October 2001 with the establishment of the Homeland Security Council. By 2004 these Homeland Security Presidential Directives (HSPDs) began to address the use of biometrics to improve the security of Federal staff, contractors and institutions with the issuance of HSPD-12, which called for a coordinated approach among all agencies to use biometrics for the identification of personnel requiring access to government facilities.⁵

The next major directive to deal with government policy on biometrics was issued in June 2008 as HSPD-24, "Biometrics for Identification and Screening to Enhance National Security."⁶ Focusing on the need to have a uniform way to use biometrics in anti-terrorism efforts, the directive outlines a "framework" to be followed by all departments and agencies in the capture, storage, use and sharing of biometric and associated data. At the heart of the directive is a requirement that agencies "shall...make available to

⁵ HSPD-12, "Policies for a Common Identification Standard for Federal Employees and Contractors," August 2004. See: http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm#1

⁶ The text of HSPD-24 may be found at: http://www.dhs.gov/xabout/laws/gc_1219257118875.shtm#1

other agencies all biometric and associated biographic...information associated with persons...that...pose a threat to national security." The directive instructs agencies to observe existing laws and international agreements on information privacy, and articulate a series of unambiguous steps to ensure that biometric data is shared as widely as possible under legal guidelines to be issued by the Attorney General. Once that guidance has been provided, departments and agencies involved in counterterrorism activities must:

- Ensure internal guidance on data collection, storage and sharing is compatible with processes used in other agencies
- Provide for interoperability between various biometric systems
- Comply with laws and policies on privacy and information security
- Ensure that the information is timely and that adequate resources are devoted to the development, operation and maintenance of biometric capabilities

Taken in context with the definitions laid down by NSTC and OMB, the extensive cybersecurity requirements of FISMA, and the historical footing of the Privacy Act, agencies faced a minefield of legal and policy mandates through which they were to thread an implementation plan for HSPD-24 compliance. The task of developing a solid, government-wide system to share biometric data throughout government was less a technological challenge than it was an exercise in tightrope walking -- especially in view of heightened congressional interest in information security.

The General Accounting Office Report

GAO issued its report entitled "Information Security: Protecting Personally Identifiable Information" in early 2008 in response to a request by Congress to ascertain progress being made by federal agencies to improve the security of information housed in their systems. The request stemmed from recent incidents in which information was compromised: the theft of a Department of Veterans Affairs laptop containing records of millions of military veterans; a systems breach by hackers that divulged 1,500 sensitive records at the Department of Energy; and another hacking incident that compromised the personal information of over 25,000 people. These were not isolated incidents; in 2006 alone, over 5,000 incidents were reported to the U.S. Computer Emergency Readiness Team (US-CERT) involving system intrusions, phishing attempts, and physical loss of portable computers and disks.

Protecting personal information while protecting privacy rights was viewed as "critically important" given the "substantial harm" that could result from the fraudulent use of such personal data, leading Congress to request a report that:

1. Identified federal laws and guidance designed to protect PII from unauthorized use or disclosure

2. Described progress in developing policies and procedures that conformed to OMB guidance

To accomplish these tasks GAO interviewed officials from 24 agencies and examined policies, procedures and plans to determine if they were in compliance with both law and guidelines. GAO would have been excused for having low expectations based on recent performance; as recently as 2006, 21 of the agencies had indicated that inadequate information security controls "were either a reportable condition or a material weakness."

In the resultant report GAO cited the requirements of FISMA and the Privacy Act and detailed the role of OMB in providing guidance to Federal agencies on adherence to information security and privacy laws. Specific attention was called to six policy missives issued by OMB between February 2005 and May 2007, dealing with issues such as designating responsibility for information privacy; requiring frequent reviews of policies and processes designed to protect privacy; recommending strategies for encrypting and protecting systems and devices; reporting incidents in which personal data was revealed or lost; and developing a breach notification policy. Agency compliance with these instructions formed the core of the GAO report. Federal officials were found to be making progress in implementing safeguards but were deficient both in adopting policies and procedures and in implementing information security requirements.

Despite the importance of those findings, the impact of the GAO report extended well beyond its intended scope. Two references concerning biometrics made it clear that there was now a common understanding of what "Personally Identifiable Information" was across government branches: the second paragraph of the document included biometrics alongside names and Social Security numbers as PII as long as such data was "linked or linkable to an individual"; and a footnote on page 5 elaborated by making it clear that this definition pertained to "any information about an individual maintained by an agency." Technologists could point to the integrity of the biometric template, cryptologists could advance new techniques for scrambling a biometric record, and systems architects could promote the merits of separating biometric data from other personal information; but with a common perception of what PII entailed now in place across these two branches of government, it was clear that any system of identification that employed biometrics had to be treated with the same sensitivity as one that used Social Security numbers to call up personal records.

Impact on Government Operations

Several agencies participated in one-on-one interviews to provide direct viewpoints on the impact that privacy laws and requirements are now having on the use of biometrics. In particular the study attempted to interview privacy officials, policy officials, biometrics program offices, HSPD-12 program offices, and any other entities with technical and policy insights on the sharing of biometric information and the deployment of biometric systems. Several agencies participated in interviews designed to elicit more information about the policy, business process, and technological challenges that might be present in the process of collecting, storing, and sharing biometric data. The goal of these interviews was to determine what commonalities, if any, exist among the insights shared by various biometrics

program offices as well as privacy officials and specialists within biometrics-using agencies. The results of these interviews were a range of perspectives about how privacy affects the process of collecting biometrics and defining the scope and abilities of a biometrics information sharing program. These views were shaped by:

1. The definition of PII and whether biometrics fall into the category
2. Agency perspectives on the sensitivity of biometrics data as standalone (i.e. not attached to biographical) data elements
3. Internal policies and procedures for completing privacy compliance documentation
4. Perceptions of privacy as a tool for either enabling or disabling the sharing of biometric data
5. Biometrics program managers' perceptions of the degree to which privacy applies within their existing infrastructure or IT system architecture

One of the initial challenges among federal agencies in understanding how privacy principles should be applied to biometrics is founded in the definition of PII. While notable federal biometrics drivers, particularly HSPD-24, encourage the use and sharing of biometric data, the classification of biometrics as PII appears at first glance problematic. As noted earlier, there are several sources in which biometrics are specifically stipulated as PII, even as standalone data elements not otherwise combined with a biometric.⁷ Therefore, while biometric usage is encouraged, any systems or programs using biometrics as data elements must ensure that all relevant privacy documentation is complete. There was some difference of opinion among interviewees as to whether standalone biometric data elements *should* be considered PII, contending that biometrics were not readily linkable to individuals, and that privacy documentation had the potential to delay agency programs' abilities to quickly implement the use and sharing of biometrics data. Others contend that the treatment of biometrics as PII ensures that all data that can potentially identify an individual is protected, and that doing so will not only provide a solution for combating potentially harmful external perceptions, but also ensure that biometrics users consider how data is to be used throughout its lifecycle. The study found that the main effort in initiating any

⁷ Office of Management and Budget (OMB) Memorandum (M) 07-16 "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" defines PII as information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. NIST 800-122 "Guide to Protecting the Confidentiality of Personally Identifiable Information," as well as the 2008 GAO Report on Protecting Personally Identifiable Information (found at <http://www.gao.gov/new.items/d08343.pdf>), validates this treatment of biometrics with the following definition: any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

program has been to ensure that biometric data sharing conforms to specified missions; that entities sharing data have the authority and legal justification for collecting, sharing, and utilizing the data; and that the receiving entity maintains sufficient privacy and security configurations as outlined in the E-Government Act and NIST standards. It was also determined that the primary issues with the collection and sharing of biometrics as they relate to privacy have largely been innocuous when initiating biometrics sharing programs.

Department of Defense

An interview with the Department of Defense's Biometric Information Management Agency (BIMA), Plans and Policy Branch, provided a range of discussion on both privacy policy and operational requirements for the collection and sharing of biometric data. BIMA described a range of ways in which privacy has an effect on its operations, from completing privacy compliance documentation to identifying sharable data sets and managing external perceptions.

First, as previously indicated, agencies are required to complete and publish systems of records notices (SORNs) in accordance with the Privacy Act of 1974, and complete a privacy impact assessment (PIA) in accordance with the E-Government Act of 2002 to identify any privacy risks present in an IT system. BIMA indicated that the primary challenge related to the completion of privacy compliance documentation did not revolve around the assessment of privacy risks or risk mitigation strategies, but rather the timely review, approval, and submission of privacy compliance documentation by privacy officials and senior leadership.

The DoD BIMA officials also indicated that a main issue with sharing biometric data is the need to have a clear understanding of the mission of individual biometric data sets and records. To comply with data usage requirements, BIMA must ensure that biometrics data that is provided to information sharing partners is done so in accordance with the stated purpose under which the data was originally collected. Compounding this issue is the collocation of biographic data with biometric data and the need to restrict access to certain biographic data elements contained within an individual record in the event that sharing partners have differing authorities that either broaden or narrow the information to which they are allowed access. In this regard BIMA acknowledges the difficulty in sharing identification records with international partners. Each of the DoD mission partners or allies has different privacy protection policies, making it difficult for commanders to share capabilities and data with their international counterparts. Specifically, commanders cannot authorize some subordinate foreign soldiers to collect biometrics because of the home country privacy laws and policies of those soldiers. BIMA is working on acquiring a policy tool which will show all of the privacy laws and policies for the U.S.'s international partners and allies. Such a policy tool would help commanders in the field to better understand what laws and policies are in place for the home-countries of foreign national subordinates.

BIMA has also encountered difficulty establishing a data sharing relationship with DHS as DHS does not have a classified database and there is concern about the effects of DHS receiving or sharing classified data from DoD (storing biographical or contextual data [see ABIS]can lead to higher classification of data).

BIMA owns the Automated Biometric Information System (ABIS), which contains biometric and biographic data collected on both blue force (“friendly”) and red force (“enemy”). Other agencies interviewed for this study maintain similar biometric databases for different purposes. FBI collects and shares biometrics data for law-enforcement purposes. DHS maintains biometrics for asylum seekers and visa applicants, among other purposes. Therefore BIMA sees its primary responsibility related to privacy as ensuring that biometrics sharing or matching that takes place is done within the boundaries of the mission for each data set, and that the technology allows for tiered or customizable access controls. The ABIS database helps BIMA avoid the conflict of storing biographical information along with biometric information because the ABIS database, with few exceptions, does not store U.S. personnel data. BIMA is looking to go into a different direction by creating a separate database called IDProTECT for “blue” force/friendly applications

BIMA also discussed the somewhat universal issue of privacy as one governed in part by perception. Specifically, BIMA must contend with internal and external concerns about information collection and sharing practices, and any negative perspectives driven by either the media or organizations that may not have an accurate understanding of the purposes – and limitations of – its programs. Overcoming this challenge requires shifting perceptions from their role in allowing somebody to do something, to *enabling* somebody to do something with the data.

Department of Homeland Security

As an agency known for several high-visibility biometrics programs as well as a strong investment and focus on privacy compliance, the Department of Homeland Security (DHS) offered several perspectives on the emphasis that it has placed on privacy during the course of administering its biometrics programs. Officials there also elaborated on the role that privacy plays both domestically and internationally when initiating data sharing agreements. A range of insights were expressed by those with responsibilities for privacy compliance, technology, biometrics, biometrics program offices, and program operations. These individuals represented the Privacy Office, the Deputy Assistant Secretary for Policy, the Science and Technology (S&T) Directorate, and the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program. It should be noted that most privacy officials at DHS interviewed for this study considered biometrics standing alone as PII, and as such, subject to the same privacy requirements as more obvious forms of PII (e.g. name, SSN, etc). This has had a tremendous impact on how proactively and intentionally privacy is considered within internal program operations, and when considering sharing programs with external domestic or foreign entities.

It was widely agreed by privacy practitioners within DHS HQ and its component biometrics programs that privacy compliance requirements – completing privacy threshold analyses (PTAs), PIAs, and SORNs – were critical for any biometrics programs to identify any inherent privacy risks. By completing documentation that includes reviews of security controls, Privacy Act compliance, and records management, the biometrics program can identify any risks in business processes and technology infrastructure up front. This enables any business process or technology requirements to be integrated into the biometrics program prior to the sharing program becoming operational. This review process gives the biometrics program managers a better grasp of what biometric or PII data is being

collected, used, or shared—and why—so that only the minimum information necessary to meet the mission needs is released.

Completing privacy compliance documentation ensures that the two critical goals of providing notice to the public and identifying any privacy risks are met in a timely fashion. The lack of documentation, or the delay in completing it, was considered by privacy practitioners to be the main obstacle to successfully implementing biometrics programs. Based on the authors' understanding of DHS biometrics programs such as US-VISIT, the delay in completing or updating privacy documentation can also have an impact on the program's ability to incorporate any particular privacy or security remedies into technical requirements for the systems that support the information sharing. One example is the incorporation of records retention and disposition schedules into IT systems to ensure that biometric or other PII data is cleared from databases, audit logs, or otherwise cached logs as required.

There are several factors that can lead to delays in completing privacy documentation. The task can be viewed as an obstacle to collection and sharing, as a low-priority cost in IT program budgets or as a complex and confusing process that can be slow or lack agility. Regardless of the root cause of these perceptions, delays in completing these requirements can delay the implementation of biometrics programs, as internal instructions specify that DHS privacy officials effectively limit the operation of any program until the necessary documentation has been completed.

A compounding issue with respect to biometric sharing and privacy compliance is the need to ensure that sharing partners meet the established baseline of privacy and security compliance established by an agency's biometrics sharing program, which is in turn defined by U.S. privacy laws, agency policies, and the results of PIAs. An information sharing agreement requires assurance that data will be protected in the same (or equivalent) fashion by the sharing partner as the data originator. This requires extensive assessment of the sharing partner's compliance posture which, by some measures, can be more time-consuming than the technology implementation to support the data sharing, particularly in instances where data is being shared with foreign governments.

From a technology standpoint DHS noted several innovations that would be useful to enhance privacy protections in biometrics data sharing. First, given that biometric data are often coupled or located with biographic data elements, there exists a need to limit or minimize the amount of biographical data that is transferred and subsequently viewed by sharing partners. This would further mitigate the need to replicate and duplicate the collection of biographical data to support validation of a biometric element with a biographic record. Some current processes are very time consuming, requiring program workers to separate biographic data elements after manually validating the correlation between biometric and biographic data on an individual. Technology that would automate this process would push biometrics program offices to be clear about what data is actually needed to specifically and directly advance its mission, and only use it in that way. It would also restrict the use, sharing, and otherwise unintended spread of biometrics beyond the purpose for which they were collected, according to DHS officials.

Second, the use of biometrics in both classified and non-classified environments creates an issue with how to quickly and effectively move biometrics information between CLASS and UNCLASS networks. PII contained within networks with different classifications are determined by the context in which it is collected (e.g. biometrics collected as part of a student exchange visa program versus biometrics collected from suspected terrorists in combat in Afghanistan). Altogether the population of individuals from whom biometrics are collected is very large, however the limitations placed on the use of the biometric due to its linkage with contextual biographic data are also significant. Therefore, it has been suggested that a technology that strips a biometric of all contextual information would effectively bridge the gap between the large volume of biometrics currently split across CLASS and UNCLASS networks.

Finally, the issue of perception again arose as a potential challenge to biometrics sharing. As one DHS privacy technologist stated, biometrics correspond in a 1 to 1 relationship with a person and as such, has the potential to elicit a stronger emotional reaction from members of the public than other textual data might because it feels like it relates to their body (e.g., there is a picture of my face, finger or eye stored somewhere where I don't want it). The fear that biometric data may reveal more about an individual than they wish to reveal, or that its compromise might represent a total loss of any unique personal identifier, can generate fear and uncertainty over the collection of their biometrics. In addition, biometrics to date have had certain social implications – for example, the stigma attached to the submission of fingerprints to law enforcement officials. The broad uses and benefits of biometrics, including fingerprints, beyond law enforcement purposes have not yet proliferated throughout society so as to minimize these stigmas.

Department of Justice

Discussions with the FBI's Biometric Center of Excellence (BCOE) yielded sentiments similar to both DoD and DHS regarding the privacy compliance challenges, perceptions, and prospective technologies. As a law enforcement entity, the BCOE and its parent bureau collect and use biometrics to verify the identities of known or suspected criminals or persons of interest using the Integrated Automated Fingerprint Identification System (IAFIS) and, as it becomes fully integrated in years to come, the Next Generation Identification (NGI) program. The BCOE also furnish labs that are designed to further the study and innovation of biometrics technologies. In addition to their explicit law-enforcement mission, BCOE also provides background-check services for pre-employment purposes.

From the BCOE's standpoint, the completion of privacy-related documentation is an insightful practice that is less disabling, and more of an exercise to keep its data collection, use, and sharing practices in check. While they faced similar issues and setbacks due to the amount of time it can take to complete and receive approval on compliance documentation (e.g. completing or updating PIAs or SORNs), all agreed that the processes were intentionally designed to generate more discussion and understanding of their information practices. In addition, the absence of comprehensive federal law governing the usage of biometrics creates some complexities with maintaining compliance however; the fallback of the Privacy Act, E-Government Act of 2002 and various HSPDs provides a sufficient framework on which to base compliance. In addition, the FBI has the ability to use its law enforcement authority to maintain, operate, and expand its biometrics program.

BCOE raised an interesting perspective on the use of biometrics – namely that during the course of completing a PIA or other risk analysis, BCOE also considers biometrics as the privacy enhancing strategy in and of itself. In other words, the use of biometrics is framed to be the solution to the privacy challenges inherent in systems intended to collect and share PII, not a driver or cause of privacy risks. In this context, it is argued that the use of biometric as a standalone data element removes virtually all privacy risks.

The future of NGI and FBI's biometric programs includes the consolidation of law enforcement and non-law enforcement data into a singular database, known currently as OneIdentity. This is similar to the future of DoD BIMA. The collocation of these two types of data sets has, however, only required the updating of Privacy Act notices and SORNs to account for the new categories of individuals and potential uses of the information. In this context, further investigation is required to determine whether or not the updating of privacy compliance documentation is sufficient to enable the consolidation of disparate biometrics records with law enforcement and non-law enforcement purposes, or if a technology solution is required to supplement.

Department of State

There are three primary entities within Department of State (DoS) that coordinate the use of biometrics: Diplomatic Security, Consular Affairs (CA), and the Biometrics for Logical Access Development and Execution (BLADE) program. While CA collects, stores, and shares biometrics on U.S. citizens' passports that link back to a central DoS database, the BLADE program utilizes a biometric identifier as a substitute for a name and password in its logical access and public key infrastructure (PKI). In order to mitigate (and virtually eliminate) any privacy concerns, the BLADE program ensures that the biometric is maintained only on the employee access card and limits the identity matching to that card thereby eliminating the need for a back-end database of biometric or biographical information, or the exchange of biometric data with other programs.,

Addressing privacy as an abstract is a challenging task to undertake as it is a personal value. The BLADE program's approach to addressing the value of the protection of an individual's privacy is to deconstruct the value into individually addressable issues. The BLADE program, it addressed the issue of the unnecessary or unintended sharing of PII by limiting the existence and authentication of a biometric to the individual's card. To address the added perception of physical privacy, the BLADE program access card takes the FIPS 201 requirement a step further by removing the biometric from the face of the card and moving it to the interior of the card.

Other Agencies

This study included discussions with various other federal officials, contractors supporting biometrics programs, identity management experts, including from NIST's Information Technology Laboratory (ITL). These discussions yielded other perspectives on privacy as it relates to biometrics, particularly the need to develop common algorithms for biometric identification that optimize performance and security. Many of these opinions, however, are predicated on the assumption that biometrics as standalone data elements are sensitive, and in fact considered PII, and as such require protections equivalent to more

conventional biographical data elements. This assumption also requires further discussion and debate in order to understand the risk that the collection and use of biometrics as stand-alone identity artifacts pose to the individual from whom they are collected, both from exploitation and identity theft perspectives.

Current Status

Biometrics as PII

Further complicating the treatment of biometrics as PII is the lack of clear guidance that specifies how privacy principles are to be applied to biometric technology or the use of biometrics data elements (e.g. fingerprint templates, facial images). While the Privacy Act, E-Government Act, OMB Memoranda, and NIST 800-122 all contribute to the framework for conducting an impact assessment and implementing controls for PII, the protection of biometric data is not specifically addressed. This proves problematic given that it is unique from more readily identifiable PII such as a name, age, sex, date/place of birth, home address, or social security numbers (SSNs), and as such may require unique protections that tailor privacy principles more specifically to biometric technologies and data elements.⁸ Biometric related guidelines and standards, including HSPD-24 and FIPS-201, do not discuss specific privacy protections, policy-based or technology-based, that can be applied to biometrics. While NIST actively works on developing biometrics technologies and algorithms, there are no authoritative SPs that address biometrics. DoD BIMA pointed out that the DISA Biometrics Security Technical Implementation Guide (STIG) and Checklist which they use to secure their systems do not include privacy-specific controls.

The impact that this can have on program managers is mixed. Some program managers elect to maintain a privacy subject matter expert as an integral part of their PM team, involving them in the earliest phases of system development or information sharing. By embedding privacy officer or advocate within the program managers, PMs have been able to complete privacy documentation and truly evaluate and address privacy risks before the program, system, and/or data sharing program goes operational. Other PMs have expressed mild confusion or uncertainty regarding the usefulness of drafting PIAs or SORNs, and the consistency-- or inconsistency-- among legal counsels and privacy officers with reviewing and approving the completed documentation. This confusion leads to the perception that addressing privacy requirements and completing appropriate documentation becomes an exercise in futility rather than utility. A unique instance that demonstrates this sentiment includes one particular agency's conduct of studies and testing of biometrics. The proposed research and testing required evaluation by both privacy officials and Institutional Review Boards (IRBs) to validate the approach and protections of PII, a process that revealed inconsistencies in the way that privacy risk assessments (PIAs) were evaluated and risks treated by the reviewers.

⁸ While the case can be made that social security numbers (SSNs) - or financial account information for that matter - in and of themselves are very difficult to link to an individual, the proliferation of SSNs across government, health, and private records and subsequent ease with which they can be linked to an individual record make SSNs as high risk and sensitive as more obvious biographical data elements.

Defining the Mission and Purpose of Biometrics Datasets

A common challenge articulated by the interviewees was the need to be able to limit data purpose and usage by sharing partners. This requires both user accountability, and technology solutions that can restrict the use of specific data sets to a pre-defined set of purposes. User accountability can be implemented using a range of solutions, from data use agreements that bind data sharing partners to data uses specified within the agreement, role-based training and awareness for users that clearly articulates how data can and cannot be used, and role-based access controls that use tiered user access to systems and/or facilities housing shared data. Technical solutions restricting data use requires looking at solutions that restrict usability of biometric data elements to pre-defined purposes, and otherwise render them inaccessible or unusable outside of a given IT system or application.

Solutions

While conducting the interviews discussed in the previous pages NBSP simultaneously conducted a paper study of emerging approaches to the next generation of privacy enhancing technologies (PETs). These include prototypes, commercially available products and white papers. (See attachment “A” – Matrix of Emerging PETs). We then selected that appeared to be four of the most promising and interviewed their developers. Those interviews are discussed below.

Commercial Off-the-Shelf Products

PerSay

PerSay offers advanced voice biometric technology that is in use by companies such as Bell Canada and British Telecom. The firm is a spin-off of Verint Systems, Inc., and has offices in Tel Aviv and New York. It offers three main product lines:

1. VocalPassword™-- a speaker identification application that can verify identity in the process of interacting with automated voice prompts
2. FreeSpeech™ -- a speaker verification system that can identify a person in the course of a normal conversation
3. S.P.I.D.™-- a voice mining and speaker identification system intended for law enforcement and intelligence use

Of the companies involved in the deployment of biometric-based solutions, PerSay is one of the few to have done so using voice-based products on a large scale. The application with Bell Canada has over 2.5 million voluntary enrollments in a system that uses the customer's voice as the password. The PerSay solutions allow identity to be confirmed either by having the user repeat a standard phrase or by employing random prompts to say specific words.

The company is developing a new version of the product to further protect privacy. Instead of storing actual audio data that can be compromised by penetrating the database, PerSay can convert the biometric template into an unidentifiable key. In this way the key -- a mathematical model of the audio track rather than the track itself or a template -- is used to verify identity.

To protect against voice phishing or recorded playback attacks, PerSay is patenting a "liveness" detection system that "combines both text dependent and text independent algorithms in the same session," according to executives at the firm. By prompting the user to repeat both standardized and ad hoc phrases, imposters who may have intercepted the user's voice cannot duplicate the requested word pattern solely through the use of that surreptitiously acquired conversation.

Biometric Based Hash Codes

Priv-ID is a European company with headquarters in Eindhoven, the Netherlands. A spin-out from electronics giant Philips, the company's core technology is BioHASH, a software product that transforms biometric data into anonymous codes that cannot be reverse engineered to compromise identity.

The BioHASH process takes a standard biometric template and converts it to a hash code using the NIST SHA-256 cryptographic hash function. The BioHASH can be stored in a database or on a card; verification is accomplished by comparing another SHA-256 encrypted BioHASH that has been generated by a live measurement against the original stored hash code. The result is a process that does not require the transmission of actual raw biometric information or biometric templates through potentially vulnerable networks. Since the hash code is meaningless without the decryption key that is used during verification, the underlying biometric information remains anonymous wherever it is stored. The small size of the BioHASH code and ability to use low-complexity algorithms to perform the matching operation allow the solution to be deployed using relatively inexpensive cards.

Priv-ID identifies three major barriers to the deployment of durable biometric-based security solutions in any environment in which privacy is a factor. The first is the "Big Brother" syndrome, in which concerns arise from having personal information and biometric data stored in multiple locations -- for example, in a health care system, a payment system, and a border control system. The end result can be a feeling of being monitored, which may or may not be true but can impart misgivings that could deter participation in a biometric-based identity management scheme of one type or another.

The second barrier is the risk of identity theft. If a finger image is compromised, it is compromised forever. A PIN code can be changed, but the image cannot. At one level the security incursion can be stopped once the discovery is made, but at another the victim is inconvenienced by having to re-enroll and establish a new biometric for identification purposes.

The final concern is that of function creep. Biometric data may exist for one very carefully circumscribed purpose, but policies can change that could lead to expanded use of the data. Priv-ID executives use the hypothetical example of the Kidnapped Queen: if a biometric database exists for a national ID card or passport application, could it be tapped to track down the kidnapper? And even if this was a publicly acceptable use, could function creep allow the database to be used on behalf of another important person in similar circumstances?

Priv-ID examined these concerns and decided to apply to biometric technology the same cryptographic hashing techniques used by banks, financial networks and IT departments to protect user passwords. Adopting this approach meant that the biometric template is converted to a random, secure set of signal

verification codes that can be stored on a card without compromising privacy. Put another way, the biometric serves as a means to generate the verification code, which can then be used by any legitimate authority to confirm identity against a separate anonymous biometric measurement.

Emerging and Developing Technologies

Anonymous Recognition

The National Biometric Security Project (NBSP) is a Washington, DC based nonprofit organization dedicated to testing, research, training and standards development for biometric technologies. In 2005 NBSP began examining ways to isolate personal information from biometric data held in large scale databases. The objective was to guarantee the privacy of enrollees while enabling the deployment of an open architecture system that could prevent identity fraud across organizational boundaries. The result, Anonymous Recognition[®] (AR), is designed to protect all PII from being compromised during the authentication process even if government agencies, financial institutions, health providers and other legitimate entities are drawing on the same biometric data to deter misuse.

Under AR, a specific subset of personal data that is maintained solely by the enrolling agency or organization is used to create a personal reference code (PRC) that is encrypted and linked to the biometric template. The submitted biometric and PRC are matched against the biometric data and PRCs in the database; in most cases the ensuing process will validate the identity of the person, but as shown in Figure A, other results may indicate identity theft or fraud. The individual or client organization retains and owns the biographic data, as well as the inquiry and disposition functions in the authentication process.

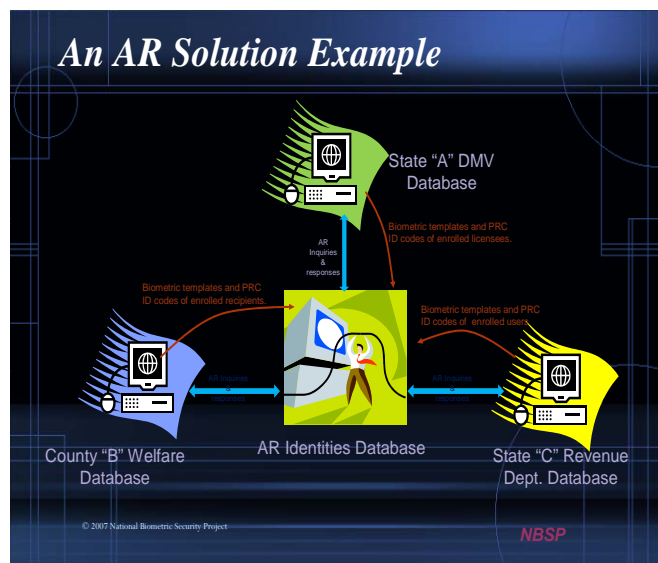
The secure AR repository is fully searchable and may contain more than one biometric relating to the enrollee. Anonymity is maintained by relying strictly on the PRC that has been derived from the

Hash	Biometric	Results
Match	Match	Previously Enrolled
Match	No Match	Potential ID Theft
No Match	No Match	New Enrolment
No Match	Match	Potential ID Fraud

individual's PII. The resultant code, or "hash," ensures that no information about the person is known to the AR authentication system; the operator of the database knows only that a PRC does or does not match a biometric in the database, or that the biometric is related to another PRC. The PRC does, however, provide a reliable pointer to any associated

biometric data. The result is an accurate, high-volume, high-speed, yet anonymous authentication process that fully protect the private information of the registrant.

A key aspect of the AR process includes having the authentication service managed



by an independent honest broker that can respond to approved inquiries. The system's multi-modal (i.e., the ability to confirm identification by examining more than one biometric associated with a person) capability relies on technologies that have been tested and certified by AR as suitable for use in both enrollment and subsequent authentication functions.

Either each time a person enrolls for the first time or has his or her identity verified elsewhere among organizations participating in AR, the PRC and biometric are used to establish an unbreakable link between the correct biometric data and the biographic information. This ability to cross proprietary databases to conduct a thorough search without having to gain access to the personal information in those databases fosters improved identity assurance cooperation among government and non-government organizations, and eliminates any opportunity for identity fraud. Under AR, as an example, states can develop special credentialing programs that can achieve the effectiveness and efficiency of a standardized format without risking access to the personal information of state citizens. The same approach is available to federal agencies that need to exercise more isolation and protection for their personnel.

The AR system is intended to meet and exceed both regulatory and practical requirements for directly addressing privacy concerns in any operating environment, including stringent Federal Government requirements for maintaining PII. NBSP executives claim that the AR solution can accommodate multiple, separately owned databases and allow common communication for anti-fraud purposes, but does not share proprietary information and is incapable of sharing private information because none is housed in the AR database. As a result, any organization can share a common authenticator without having to reveal sensitive data.

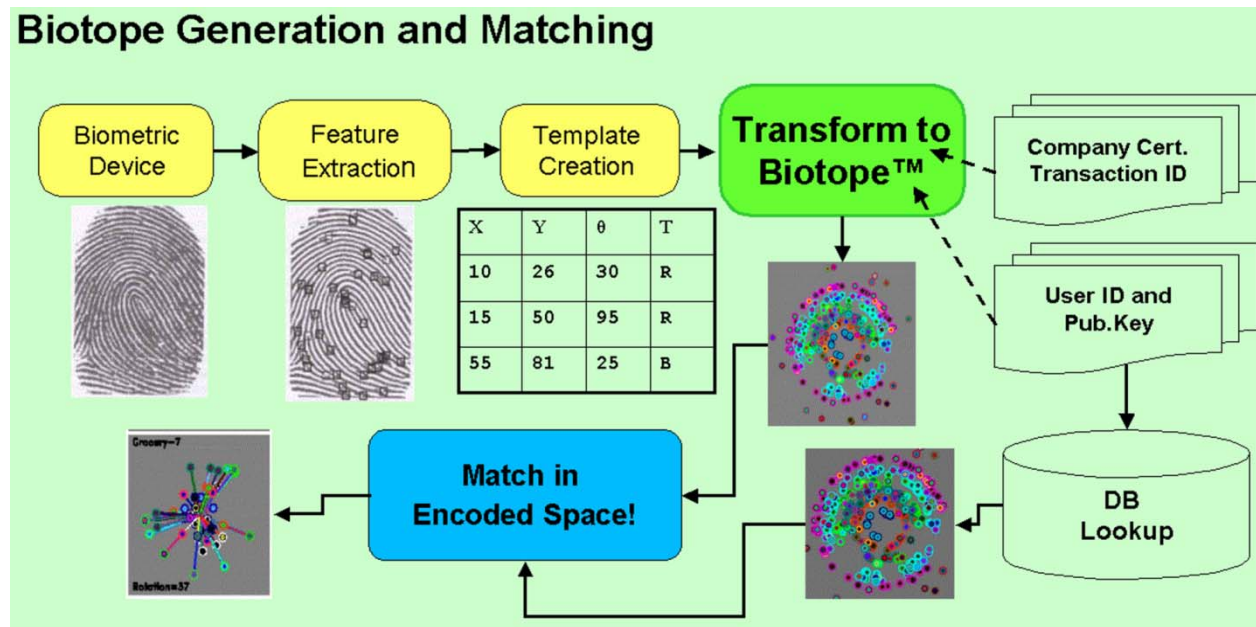
Revocable Biotokens

Securics, based in Colorado Springs, Colorado, was founded for the purpose of assuring that biometric-based identity systems could operate without threat to the privacy of enrolled individuals. Its core technology, Biotope®, uses revocable, irreversible biometric tokens to ensure that the end user can control the use and spread of his or her biometric information. Cryptographic protocols are used to ensure that the generated token is unique for each transaction. The company claims that this process of new real-time tokens makes network transactions impervious to key exchanges, phishing, and other types of attacks.

An interview with Securics co-founder Terry Boulton revealed further details about the firm's approach to solving problems arising from the mere existence of a biometric database that, if hacked, can have serious consequences in terms of both security and privacy. Boulton uses the example of a spoofed finger image being used to penetrate an ATM network as one type of fraud that does not have to occur very often to cause widespread mistrust of a system that relies on biometric verification to complete a financial transaction of any sort. Despite such concerns, biometrics still have a significant role in certifying the authenticity of each transaction. A public key infrastructure may confirm that the machines on each end are legitimate, but depending on a user ID and password based authenticating mechanism is becoming increasingly risky in the face of sophisticated attacks.

Using biometrics to verify identity is an obvious solution, but additional steps are necessary to make certain that the biometric being used at the other end actually belong to the person involved in the transaction. Otherwise the transaction would be open to compromise through the substitution of a biometric somewhere in the network, or through the use of what Boulton calls a "doppelganger" technique. In the latter instance, a biometric database is searched for a double -- someone whose stored biometric matches that of the attacker -- and that newfound identity is used for a fraudulent transaction.

The Securics innovation that gets around the dilemma of needing biometric-based identity assurance without creating privacy concerns is the Biotope[®] token. The Biotope[®] is derived from a combination of the biometric data, the company ID and key, and the user password and public key. The biometric, authorized for use in the transaction by the user password, provides two factor authentication. Unlike other solutions that store both of the factors separately, the Securics process stores both together; one factor cannot be used without the other to generate the token. In addition, new tokens can be derived from the original token and new keys imbedded within each succeeding transaction.



The significance of being able to generate new tokens in this manner is that the token may be revoked -- that is, canceled by the user or the system operator -- without having to re-enroll the person's biometric in the system. Instead, re-enrollment consists of taking the old token, deriving new data from it and then reusing the same biometric. The technique protects individual privacy, yet also provides the administrator of a hacked biometric database with the tools to generate new tokens without having to re-enroll all participants. Securics calculates that this process of combining all of the keys generates a token that is statistically impervious to brute force hacking; an insider would require 2^{108} operations to break the token, and an outsider would need 2^{120} steps to successfully attack it, assuming the intruder could solve one step that has no known algorithm.

Securics adds another step to secure the biometric-based token, or "biotoken," by combining stable biometric data with additional reference points that can vary within known parameters. Without divulging proprietary information on how this is done, Securics executives give an example of a person's height -- something that may change from day to day based on stance or shoes -- as a way of introducing a definable variable, i.e., one that may be somewhat inconsistent but nevertheless can be measured within a certain "window" each time. Since neither the variable nor the window are divulged, an additional layer of security and accuracy is incorporated into the biotoken.

In operation the Securics solution starts with the creation of a strong root ID that is generated from a biometric. The root ID serves two purposes: first, it is used to search for matches within the database and ensure that the identity is unique; and second, it forms the basis for the creation of derivative identities that are unique to each application, e.g., one for banking, one for worksite access, and another for border control. The existence of an application-specific identity coupled with the ability to generate a highly accurate bipartite (i.e., a combination of the stable biometric and unstable variable) biotoken from that identity establishes an environment for conducting secure transactions over inherently vulnerable public networks such as the Internet. This is accomplished by not having to transmit the actual biometric data; instead, transaction-specific biotokens are generated at each end of the process to verify identity.

In practice verification may be initiated by sending an authorization request to a server that stores or has access to one of the base identity tokens that have been derived from the root ID. The server takes the base token, a transaction ID and a policy authority (PA) key to generate a bipartite Biotope that is unique to the transaction. The Biotope and the transaction ID are sent to the requesting site, where the locally captured biometric is used to generate a separate token. The local token is compared to the one received from the remote server, and the results are sent back to the server in the form of an authorization ID and a nonce key that is derived from the Biotope matching process. Securics asserts that this solution solves both man-in-the-middle and phishing attacks because none of the data -- even if transmitted with no encryption -- has any further use. The bipartite Biotope cannot be reused, and no raw biometric information is being transmitted by either party to the transaction.

Conclusions

The purpose of this report has been to:

- Document the legal and regulatory environment in which Federal agencies must operate when implementing programs involving the use of biometrics
- Examine procedures currently being used to ensure compliance with those laws and directives
- Point to technologies that may help overcome some of the barriers to deployment and, higher on the complexity scale, data sharing

This latter imperative of being able to move information between agencies is at the heart of some of the most ambitious government-wide projects announced in the past decade: HSPD-12 calling for a

common system of identifying, documenting and exchanging information on Federal employees and contractors; and HSPD-24, mandating the adoption of a uniform framework for agencies to capture, store and share biometrics in an effort to deter threats to national security.

Both of the far-reaching directives were issued amid a daunting array of requirements to protect privacy, dating back to the Privacy Act of 1974. FISMA legislation in 2002 provided specific guidance on how any government held information must be subjected to exhaustive measures designed to prevent unauthorized disclosure. Placing further pressure on officials charged with introducing biometric systems into agency operations, both OMB and GAO announced that biometric information -- whether linked to other biographical data or not -- was to be regarded as Personally Identifiable Information (PII). The basis for this determination is uncertain; as noted elsewhere in this report, biometric templates alone say nothing about the person with whom they are associated and have proven resistant to hacking and forgery. Nevertheless, the linkage of PII and biometrics became a given that dramatically affected implementation efforts. As we put it on page 4:

The challenge faced by government agencies is to determine the right combination of technical solutions, policies and implementation practices that maintain an effective barrier between biometrics and other forms of PII, yet enable the use of biometrics in critical programs to prevent terrorism, identify criminals, safeguard the warfighter, protect government facilities, and provide innovative services to the public.

We learned in our interviews with the most affected departments that agencies have been innovative in straddling the line between data protection and system deployment. To expedite compliance with FISMA in particular, privacy experts have been embedded in the project framework to ensure inordinate delays are not encountered as the implementation date approaches. Programs that are intrinsically multi-agency in nature also face the hurdle of having to separate agency-specific data from that which may be shared in spirit with the requirements of HSPD-24. To meet those goals officials have adopted labor-intensive processes to cull information that cannot be subjected to external disclosure. These include creating systems of records notices (SORNs) in accordance with the Privacy Act; conducting privacy impact assessments (PIAs) per the requirements of the E-Government Act of 2002; and privacy threshold analyses (PTAs) as mandated by both the E-Government Act and the Homeland Security Act of 2002,

Meanwhile private sector entrepreneurs have been focusing on ways to segregate, conceal and encrypt biometric information to ease the process of moving identifying data from agency to agency, of confirming identification without requiring the release of a biometric template, and of disguising the biometric to insulate it from compromise. The resultant products and concepts take into account both of the variables that must be considered for any government-wide program: first, solutions must be technically able to safeguard the data; and second, they must withstand the scrutiny of other interested parties who are skeptical about any government use of such information to prove identity.

The four technologies selected for examination in the report meet these criteria. Used alone or in combination, they offer an opportunity to achieve operational goals without risking unauthorized disclosure. The Priv-ID BioHASH® provides a means of using a biometric as the basis for generating an encrypted hash that may be safely transmitted without risk of exposing the underlying biometric. The technology is highly analogous to security measures used by financial institutions to protect sensitive information. The ability to use biometrics at either end of a transaction without having to relay the template across potentially unsecure networks expands the range of applications for which biometrics can be a component without being a risk factor from a privacy standpoint.

The Anonymous Recognition® process developed by NBSP demonstrates how biometric information can be used to prevent identity fraud across organizational -- and even sector -- boundaries. Participating entities can load biometric information into the AR system, where a personal reference code is generated to link a known identity with the biometric. AR never knows the identity of the registrant, but nevertheless can validate or repudiate an identity based on the link between the personal reference code (PRC) and the biometric template. Privacy remains intact, yet disparate organizations may query the database to make sure a new employee, contractor or customer is associated with the proper identity.

The Securics Biotope® solution takes yet another approach in protecting the integrity of the biometric verification process without actually transmitting biometric data across networks. Developed out of concern that a biometric could be discovered and then substituted somewhere along the network (the "doppelganger" vulnerability described above), the Biotope® combines multiple factors such as a biometric, a company ID and key, and a user password and public key to generate a hack-proof token at both ends of the transaction. Each token is unique to the event, making it useless for future transactions. In practice the Biotope® process can be used to verify identity in high volume, real time environments without having to transmit an actual biometric template.

PerSay offers another option for using biometrics as an enabling technology without having to subject the data to compromise. Using nothing more complicated than a telephone connection, PerSay captures a voice biometric template, converts it to an unidentifiable key that is a mathematical model of the template, and uses the key to validate identity when the speaker repeats a known phrase or responds to random questions. A "liveness" function further reduces the chances of an imposter using an established identity.

In Summary

This analysis has examined the three main dimensions that influence the development, deployment and use of biometric solutions in government programs: the complex and often contradictory legal, regulatory and policy components that dictate how the programs are to operate; the procedures being developed by government managers that enable them to introduce new systems that are fully compliant with all such guidance; and the products that can isolate biometric information from abuse yet make the technology useful for validating identity in a variety of operational environments.

The process has yielded several conclusions:

1. The Privacy Act, FISMA, and the OMB/GAO determination on what constitutes personally identifiable information profoundly affect the design and operation of any government program that uses biometrics to establish and validate identity. In particular, the HSPD-24 requirement to exchange biometric information for the purpose of identifying those who may pose a threat to national security has resulted in agencies having to develop labor intensive procedures to ensure that disclosures are managed within the existing legal and policy framework.
2. Government managers have been creative in finding ways to avoid operational delays stemming from meeting compliance requirements of FISMA, the Privacy Act, the E-Government Act and related intra-departmental guidelines. Techniques such as embedding privacy experts in the project development phase have overcome some of the barriers that would have delayed or even imperiled data exchange programs that are vital to national security.
3. The complexities associated with being able to set up government-wide identity management systems for workers and contractors has indefinitely delayed implementation of the key provisions of HSPD-12. While most departments have taken steps to adopt standard procedures for recording identities and issuing identity documents, full realization of harmonized practices and seamless data exchange across agency boundaries remains a goal rather than a reality.
4. Products exist that would ease the burden of meeting, for example, the contradictory objectives of FISMA and HSPD-12 compliance; however, none of the technologies identified herein have been brought into use. Limited trials might establish the viability of these and other innovations to address challenges in maintaining database and network security of biometric information. Similarly, agencies have yet to identify needs and seek solutions that are tailored to specific biometric security requirements.

The short list of technologies covered in the report were selected on the basis of their potential ability to help agencies navigate a difficult path -- one that straddles both the compelling need to implement biometric-based security systems, and to meet legal imperatives on data protection. This is not meant to be an exclusive list; certainly other efforts are being made to develop effective ways to insulate sensitive information from unauthorized access. Those elaborated on above, however, were found to be illustrative of the technological progress that is being made in this area. One rises to the challenge of being able to validate an enrolled identity across departmental boundaries in accordance with HSPD-12; two others demonstrate how existing biometric data can be used as the basis for real time verification without having to transmit an actual biometric template; and another shows how even the most rudimentary infrastructures can be leveraged to perform identity matching chores when no other option is viable.

Government officials are confronted with imperatives to deploy effective biometric identification systems without raising legal, ethical or perceptual concerns about privacy. Based on the research

outlined in this document, it is likely that this challenge can be met with solutions that are either available in the marketplace or can be customized to suit most field operational requirements.

Appendix "A" : Interview with Mr. Almog Aley-Raz, President of Per Say Inc.

Representing NBSP, Mr. Russell Ryan, Task Manager, Mr. Gerald Williams, Consultant to NBSP, and Mr. Justin Smith, Technical Representative.

PerSay is a leading provider of advanced biometric speaker verification products and one of the first companies to integrate next generation privacy enhancing technology to voice biometrics.

NBSP: This is Russ Ryan and Jerry Williams and Justin Smith.

Aley-Raz: Hi.

Aley-Raz: Yes, Almog is my first name.

NBSP: All right, I am Jerry Williams and Russ Ryan is the Task Manager working on this task and Justin Smith is our Technical Representative. Russ Ryan is probably in the best position to give you an overview of what we are trying to do with this project and for whom, so I will defer to him as he can provide an introduction.

NBSP: Thanks Jerry. The overview is actually is fairly well explained in Jerry's original e-mail to you sir and as part of one of our government contracts, we are tasked with reviewing the impact privacy may or may not have among government agencies and departments with respect to either sharing biometric data or the storing of the personnel information that's acquired at the time of the biometric capture.. So part one of our task is really to spend time with the appropriate privacy officers from DOD, DHS, Justice and other government agencies to try to discern the key issues, where are the pain points.. Secondly, we plan to look at the various initiatives that are taking place at an ever increasing rate with respect to the development of newer and more privacy enhancing biometric technologies. Jerry is leading that effort and has developed a matrix of forty or so initiatives. Some which range just from white papers to those that are nearing commercial development or just coming on commercially. Having done that we identified a number of what we thought would be the most appropriate ones to

start off with because they seem to be closer to the marketplace or already in the marketplace such as yours. So the second part of our task is to identify what we think are the most promising technologies, describe what they do, describe their approaches to privacy enhancement in the biometric arena so that government officials, privacy officials in the US government and quite frankly in the private sector as well, can get a better understanding of which of the approaches are best going to suit their particular requirements with respect to the issues they may or may not be having with privacy. .

Aley-Raz: Yes, I perfectly understand the issues around privacy and biometrics and actually I have been speaking in a couple of conferences about them. I have met Ann Cavoukian from the Ontario's Privacy Commission as well as the Israeli commission and yes there are some challenges and issues and you know they are not quite the same for every biometric, but the concerns are you know well appreciated.

NBSP: Yes the federal government has apparently if not decreed at least accepted the concept that a biometric template is Personally Identifiable Information or PII for short. That means that anyone who has a biometric template must protect it and we identified a number of people who are trying to do that and we winnowed them down to what I termed "Credible" potential solutions. Credible meant we could find such a technology advertised on a website as a commercial offering or someone had developed a patent or been issued a patent which sort of gives a signal that they are moving from the theoretical to the practical commercially developable product. Much of what was in the matrix were just research articles, but we have identified three "credibles", plus a patent and it came a little bit of surprise to me when two of the three are using the ideas of priv-ID. At the time I believe you probably formed an association with them, they were members of Philips and they spun off a company called priv-ID. So we wanted to talk to you and find out a couple of things, I have got maybe ten questions to ask. But I would offer you this opportunity to talk to us about any general things about your technology or maybe even about the project you developed with BellCanada and then I can go through the rest of my ten questions.

Aley-Raz: All right, so first of all if you have heard about Per Say. We are one of the few companies that actually focused on voice biometrics and the only one to successfully deploy this in large scale customer facing deployments. We have deployments in five vertical markets: fashion services, telecom operators, healthcare service providers, large enterprises for all kinds of internal employee session application. As well as the government, police and intelligence agencies I mean worldwide. Per Say has both text dependant and text independent technologies which can be used in various ways and the basic input to these systems are voice recordings and in some voice recording contain a password, which doesn't have any content in terms of privacy. At Bell my voice is my password so it's not like you are talking to the bank and issuing a transaction by providing some sensitive information. You know, recording of customer talking to a bank agent which in most of the cases do contains some sensitive information and so we are facing regulation in many countries which sometimes prohibits the storing of biometric information. Many of these regulations contradict existing regulations in financial services, I mean if you record the call for audit trail I need to keep it for seven years and you know this is biometric information.

So on the one side you have to record it, on the other side from a privacy perspective in some countries you can't, but you know the reality that the, you know the banks collect my hand signature, my voice, you know the picture of me and there are some contradictions there. My point of view is that the biometric information is basically from the public domain, I mean it's just spread all over the place. Nonetheless Per Say is a biometric company, it's not a speech company and as such we understand the sensitivity and we will differentiate Per Say from other players in the voice spaces that we view ourselves as a security company and we invest significant resources from our side to protect information that is stored in our systems and we look at the common criteria protection profiles for biometric systems and then try to derive the requirements for our products. And we undergo security audits by our customers which are mostly banks and government agencies so we are in this space.

With any of the biometrics, the actual template is just a bunch of binary digits and it doesn't have any privacy related information in it, I mean if you actually decode our encryption and get your hand on that template you can't do anything with it. There are several layers of protection with that information but in a sense they are useless because even if you have it you can't do anything with it, it's not the audio. So it boils down to storing audio at the end of the day and the storing audio sometimes as I mentioned do contain sensitive information sometimes, no. We are participating in one of the **ISO** committees and we are a contributor to the voice XML forum about finding the standard way to store audio. And as far as I know the industry has yet to find a protected way of storing the audio because every scrambling is proprietary and basically storing audio is something that most of the contact centers do, sometimes for quality assurance, sometimes for the other purposes for audit and in our case for creating voiceprints. So, at least from my perspective, I don't see them as something that is as sensitive as some of the agencies do.

Now as far as the project with priv-ID we are at the point where we deployed our system at Bell Canada and we have the largest customer facing deployment there with somewhere in the range of two point five million voluntary customer enrollments and since Bell has their own privacy officer, we were introduced through Bell to Mrs. Cavoukian and she was deeply involved in biometric encryption at the time. I am sure that is still the case and one of her ideas was to try and implement the biometric encryption to a voice biometrics.

Basically the whole idea is to instead of having a template that is proprietary and is stored in a system and one can use there some kind of an encryption mechanism that's mapped and the voice template meets with keys and that key can be scrambled with additional information and can be revoked, in a way that it enables the people who are very sensitive to privacy and do think the template itself can be reverse engineered to actually transfer in an unsecure manner. So for example if we have a voice biometric system in the Bell premises and the authentication is done in our servers you could think of maybe when a customer wants to enroll I can send him a copy an encrypted copy or a key to his device and do it locally without that being concerned about, this being intercepted and used to breach some kind of a privacy law.

PerSay has developed an engine, which looks like a voice biometric engine. On one side it gets an audio file or files that contain the person's voice and on the other hand it produces a key that can be used for further verification. Now we were quite amazed by the fact that our templates, which contain somewhere in the range of fifteen kilobytes of information, can be mapped on to a 128 bytes of the key, without significant degradation and performance though there is some degradation. With voice, if you are looking at an equal error rate of one percent and that degraded to maybe one or one and a half percent by doing that process, but still in concept it shows that this can be done. Now we haven't done further investigation since that exercise which was completed about a year and a half ago, the guys from priv-ID you know were busy with their spin-off from Philips. We were busy with survival and getting additional customers. But today our company is doing quite well and we see a spike in the adoption of voice biometrics and I believe it's going to be one of the most popular ones as you don't even need specific device to use it. So coupled with the fact that voice is applicable across all communication channels; you can use it on the web, on the mobile, on the voice channel it is probably going to be one of the most popular ones used in commercial industry.

NBSP: Okay, thank you for that overview. You probably wouldn't remember what specific directives, laws or regulations that you meet. I mean you said it varied by country and that's not an important question anyway.....

Aley-Raz: I can tell you for example that Greece, is drafting with the Hellenistic Privacy Protection Agency something that says: "We don't want you to store the audio because it's not allowed." And once we got into an engagement with them and explained the technical aspects of our process, they waived that requirement. Our customer explained to them that, they are using their own password, and that recording is not really a threat or a risk, if it's kept in the bank in the way other sensitive information is, they'll have to live with it. Nonetheless in our upcoming product versions there is a transcriber mode that is audioless, so yes we use the audio but we don't store it anyway on any disc and that enables us to actually overcome such requirements, but we think that if you don't store the audio, the original enrolment audio, you will have a problem once newer and more accurate algorithms become available. So we only recommend to our customers to please store the enrollment audio in a protected manner. When we do the storing in our system it is encrypted, it is hashed, it is by that specific sites key, so even if you have it, it won't work in any other space or systems.

NBSP: You essentially can store and transmit an unidentifiable key I think as you said, but it does not include the actual voice biometric template?

Aley-Raz: Yeah, basically it's bands of numbers that are related to our specific technology and they are mathematical models of your audio generation system.

NBSP: And if that were ever grabbed by someone, a hacker or something you could revoke that and create a new one with the same voice biometric is that true?

Aley-Raz: Yes, the project that we did with priv-ID, demonstrated that capability. In fact none of our customers uses this engine, as it is slightly less accurate than the state of the art, but in concept that can be done.

NBSP: Okay, is there any threat from someone listening in on a transaction between let's say a bank and you and using that as a playback attack? Simply record the voice of the subject and then provide that same voice recording back to the institution, claiming to be that person.

Aley-Raz: With the text, we are authenticating bank customers in two areas. One, when they are interacting with the voice response systems and secondly in the background of a natural conversation in real time. We can also do a real time fault through detection as people are speaking with agents. Now in terms of the human to agent conversation, you can record it, but you have got to do it very, very well so our customers don't perceive that recording risk as a serious one. In the interactive voice response systems certainly recording threats whether through interception or through what we call Vishing, or Voice Fishing. We must address them in several ways. One way is to use prompted passwords, which randomly prompt the users to say specific words. We don't believe that digits are good because they are not secure enough and can be arranged in any order quite quickly. But if you use some item of speech and randomly ask for sequences that can be secure enough. On top of that Per Say has actually submitted a patent for its livenessdetection system which combines both text dependent and text independent algorithms in the same session. Basically we use a static phrase which is the most accurate way of authenticating people or speakerstoday, and immediately thereafter prompt the user for a random phrase and now we check the users which didn't get the phrase and in parallel what we are doing is creating "on-the-fly" two voiceprints from the two utterances which are in effect independent, and you know check basically that the record is coming from the same person. So there is some kind of exposure to recordings and some of these can be mitigated by giving the right call flow and using the technology in a way that minimizes the risk.

NBSP: Priv-ID has advertised, their "Ashara" biometric encryption ID card solution where there is no database at all and the matching occurs right on a card. Is that in any way similar or is it totally different than your application with Bell Canada?

Alay-Raz: Bell Canada doesn't use their biometric encryption. The project through the introduction of Bell Canada did it includes the actual system that runs there is using standard encryption of templates and just the way most of our customers do. And the priv-ID exercise proved that the voice can be mapped on to a key which can be combined with some additional information that it can be a result and that's a – it can be the exact same way they are doing each for voice, for fingerprint. Nonetheless, you pay a price in performance and accuracy by doing so, with the experiment done so far. They are doing here for a live research as our basic algorithms are you know actually a fusion of several different approaches. We only took one of these approaches and integrated it in the project. So today if we are to develop an engine to get with priv-ID's that they will generate those keys which can be distributable, there will be some degradation of the verification accuracy, so there is a trade off here.

NBSP: Okay, I noted on your website that you said you had a third party security expert do a rigorous evaluation of your system. What was the nature of that evaluation and is it possible to see any written results of it?

Aley-Raz: Our bank customers in Israel and elsewhere take our systems to third parties, or their own security experts. They review and audit the system security, try to break it and hack it. I mean the most extensive tests were done which we are exposed not to all the customers, we are exposed to what they are actually doing. They were done here in Israel so their report is actually in Hebrew. Now when we underwent this process with Key Link for example, we just got a couple of rejects which they wanted us to fix and but that was it. We do have a security overview of our system which I can share with you and besides that we are just utilizing, not inventing security and not inventing encryption, we are just using it and obviously we think that we protect the data in our system. So for example all the biometric information of the template is stored in active directory where you can control access to any entity in any level and since we are writing on a windows platform we use integrated windows security as far as these security is strong. Now in terms of the encryption we use the standard encryption mechanisms in signing of voice templates with specific local keys. I mean we have to protect our systems from the DDA's and some other people that are system administrators. We have role-based authorization so we can control, who can do what and any smaller features and capabilities that they all together provide a comprehensive suite of protection through the system against the various threats.

NBSP: Well anything you could share with this, without endangering yourself or violating anything would be very much appreciated, you could send it to Russ Ryan or you could send it to me directly and anything you feel appropriate would be most welcome.

Aley-RazThis information is shared with every customer. So you can make sure because this information doesn't drill down to the bits, it's just an overview showing all the mechanisms. If you need any additional information besides the overview that I have shared with you, you just let me know.

NBSP: Well, let me explain to you what we will be doing. We will take the information that we have gotten here and we will summarize it and we will continue with a couple of the other interviews and we will keep you apprised as we move forward and the project is progressing, and we may come back with additional questions from time to time. We also realize your travel schedule is really hectic so we appreciate you taking time out for us to have this conversation.

Aley-Raz: All right, my pleasure.

NBSP: Thank you all.

Appendix “B”: Interview with Mr. Michael Van Der Veen, President of priv-ID

Representing NBSP, Mr. Russell Ryan, Task Manager, Mr. Gerald Williams, Consultant to NBSP, and Mr. Rick Norton, Technical Representative.

priv-ID is the leading provider of PET (Privacy Enhancing Technology) that eliminates privacy and security concerns in biometric deployments. The company offers the high-quality [BioHASH® solution](#), which stores and matches standardized fingerprint information using an irreversible binary hash code. The same hash technology is routinely used in securing PIN codes in financial transactions and passwords in IT security]

NBSP: Mr. Van Der Veen?

Van Der Veen: Hello.

NBSP: Hi, this is Russ Ryan, how are you today?

Van Der Veen: Hi Russ. Good, thank you. How are you?

NBSP: Very well, thank you. I have two colleagues on this call with me, a gentleman by the name of Rick Norton and also, another gentleman by the name of Jerry Williams.

Van Der Veen: Okay, hello.

Van Der Veen: Yeah. Where are you calling from?

NBSP: I’m calling from the Washington DC area, Rick is in Colorado and Jerry is in New Jersey.

Van Der Veen: So you have the whole world presence?

NBSP: Yes, we've got a lot of time zones covered. Anyway, you saw my original email so you understand what we're trying to do.

Van Der Veen: Yeah.

NBSP: And as I think I explained in the email, Jerry has done a lot of the work on this, a lot of research on privacy initiatives that are taking place, you know, within the biometric area.

Van Der Veen: Yeah.

NBSP: And he has come up with a matrix of quiet a few, many of which are just at the whitepaper stage as opposed to actual technology and development, what have you. But obviously, the works that you are doing, that was one of the ones that was really nearly the top and what we wanted to try to do was to at least have a first conversation with you and try to understand your technical approach in what you're trying to do. Our end result of this effort is to be able to do two things; one, publish a paper that articulates the concerns privacy is causing, especially in the US Federal Government Departments with respect to sharing information and also, with respect to the amount of resource it requires to protect the CII that's captured along with the biometric, and secondarily, be able to point the government to various technology approaches, such as yours and others, that describe the differences in those approaches to give them a better understanding of which of them will probably be the best to help them, okay?

Van Der Veen: Yeah.

NBSP: So we started looking at your Ashara Biometric Encryption ID Card solution.

Van Der Veen: Yeah.

NBSP: And a question I have is- is that the same solution that you were referring to in the presentation you gave in London, last October, where you had the multiple and different encrypted encryptions taken off of the same template or image.

Van Der Veen: Let me give a very short introduction. You know of the relation between Philips and Priv-ID, because I used to be a former Philips employee and Priv-ID is actually a spinout from Philips. We were spun out from Philips in 2008, and we were the lucky company that got all the IPR and all the technology on biometrics that was done within Philips and we took that along with the company, Priv-ID. So basically, you could say the initiative that we did with PerSay at that time, I believe it was 2007 or 2008, was done under the Philips flag but was based on Priv-ID technology. The technology that we have is... actually, we have two different names for that; one is Ashara and one is BioHash. Ashara is, for us, a tool with user interfaces and an enrollment facility, you know, and all the things that you require for a successful biometric deployment. But the key technology that is used in Ashara is called BioHash. So if we're talking about software to protect the security and privacy of the biometric information then we're talking about the BioHash technology and not ParSay, the Ashara technology; but that is merely a naming convention. I'm a little bit, looking into the vision into the future, it's my personal vision; and if you look at large scale deployments, large scale biometric deployments then these come with a number of privacy concerns. And I think basically, you can categorize them in three different ways. First of all,

one of the privacy concerns that you hear all the time is the “Big Brother is watching you” argument; biometric information is personal, identifiable information, and by storing that in multiple locations, it that means actually, that in a payment system, and in a healthcare system, and in an e-passport and in border control settings and everywhere you go, you have personal identifiable information stored; you have your biometrics stored. And that can create a feeling of “the Big brother is watching you. ” The second, and that, I think, is a more serious threat is the risk of identity theft. Imagine that you would only have one single entity, one single database in which you store the biometric and then you can put all the measures in place to protect this database. But what is happening today is that biometrics is being used on multiple sites; it is being used for payments, and it’s being used at border crossings, it’s being used everywhere. It means that, if, in one of these locations, the biometric is compromised, it is comprised for all the other applications, and it is compromised for all the other applications because you only have a limited number of biometrics. So if your right index finger is compromised you cannot simply renew your right index finger; it’s compromised forever, so to say. And that’s a clear difference with pin codes. If you lose your pin code or your pin code is stolen or compromised or whatsoever, that is not so nice but you can issue a new pin code. And if you have a new pin code then you’re in business again; that is not possible with biometrics. So there is a fundamental difference in that. And I think if we want to use biometrics on a large scale in the future then we should take very good measures to make sure that we don’t end up in a mess, so to say. I think the last part of the concern, so that is the third one, is the risk of Function Creep. And Function Creep is where you create an application that is intended for one purpose, and that the purpose is extended. And I can give an actual example that is happening in the Netherlands; in the Netherlands we are discussing on... we have e-passports and the Government has passed legislation to also store the biometric information in a central database. And the purpose for storing biometric information in a central database is to find duplicate checks, so to find frauds in applying for passports. The government, at this moment, guarantees that the biometrics will only be used for that purpose, so that is fine. The risk now, is that this policy can change, and we know that every four years the government changes; this database is there and so also, policies can change. Policies can change very quickly and they can maybe... let me give you an example, take our Queen; in the Netherlands, we have a Queen. And suppose our Queen is kidnapped and the government had a policy that this database which is there, which contains all the fingerprints of all the citizens in the Netherlands is there. And then you have a valid question, “Is it now allowed because the Queen was kidnapped, to make use of this database and find the person who kidnapped the Queen?” And I think if you asked all the citizens in the Netherlands, 90% of people would, “Yes, it’s allowed. ” And that is actually, the start of the Function Creep, because then, suddenly, it’s not the Queen who is kidnapped but it’s another important person. So there is a gray area in this and policies may change, and that risk leads to a much wider use of the same database, and that, again, leads to the spread of identity theft. So I think, looking into the future, we have to be very careful in rolling out biometric systems in a successful way. I mean, we have successful point solutions now about one step growth. It can easily end up in a mess and we should prevent that.

NBSP: It was interesting that at the conference, you were one of the participants in the Privacy Panel and it seemed one of the most difficult questions that the panel was asked was how to define or describe privacy?

Van Der Veen: Yeah. That is, indeed, a difficult question. And you have, to do have a real solid answer to that, you have to look at the attack model in biometric systems, I would say. If you have a biometric deployment and you have the possibility to use a spoofed finger, you know, then you have a way to circumvent a biometric system, whether there is privacy or not? In our definition, privacy is associated

to storage. So wherever the biometrics is stored, either on an ID Card or in a database, make sure that if this database is compromised that the data that is contained in that database or in the ID Card cannot be used to reconstruct the bi-metric information and cannot be used in other applications than it was originally intended for. And I think once you achieve that then you also address the privacy concerns that were mentioned earlier; the risk of identity theft. So for us, it is very much related to the storage of the biometric information. And, of course, you have other things there, you have things like spoofing, and you should address that; but I would say that is a different topic.

NBSP: I would agree. That's more of an attack on the system, itself, than the privacy.

Van Der Veen: Exactly, yeah.

NBSP: I know when Jerry was looking through some of the information on your product, he had some questions about it, and I was wondering if these are some that we could discuss with you now or?

Van Der Veen: Yeah.

NBSP: Alright, good.

Van Der Veen: Sure.

NBSP: Jerry?

NBSP: Well, I think, probably, you've already addressed my first question on the list. And the question was, when you say Ashara is privacy compliant what do you mean? And you have provided a definition, a practical, pragmatic definition as to what it means to you, and that is making sure that this biometric cannot be reconstructed from what the perpetrator obtains. Did you or have you aimed at any specific directory, the directives of laws or regulations in developing the technology, that you said "Yeah, this complies with that regulation"?

Van Der Veen: We have. And because our definition of privacy is not something that we invented, but we are carefully looking at the standardization activity within ISO; there is an ISO standardization activity going on in SC-27, and that is Project-24745. And in that ISO standardization activity they are looking at all the legislations that are available. And in that standardization, they come up with a definition of what is privacy and how we make sure that in a biometric system we can work with a kind of, referenced architecture in order to address the privacy concerns. And the privacy concerns that are mentioned there and that are taken from the various legislations that are there are in terms of irreversibility, renewability and unlinkability, confidentiality and things like that. So, yes, we have and, yeah, we carefully follow the standard which is in progress on that point. Have you seen that standard?

NBSP: No. Did you say SC-27?

Van Der Veen: Yeah, it's SC-27 and then Project-24745. Maybe I can explain one level more in detail about BioHash because that'll help you understand how that works.

NBSP: : Yes.

Van Der Veen: It works very similar to the way how we protect pin codes and passwords. If you log on to your computer you have to type in your password, and that password is compared to a password that is stored in the system, on your PC or in the network. For security reasons, the actual password is not stored but it is encrypted, and there is a special type of encryption used, and that is a one-way encryption tool and that is called a Cryptographic Hash. And a Cryptographic Hash has the property that you can encrypt it only in one direction; there is no pin involved and it is impossible to go back. So that is a common technology that is used also, in the banking sector, in the financial sector and in the IT world. And the same technology, the same security technology, we use in biometrics. And that means you take a biometric sample; so you have a fingerprint scanner and you put your finger on the scanner and you get a fingerprint sample. And from that fingerprint sample, in the same way as you protect a pin code, you use the same security tool to protect the biometric sample. And by doing that, you do not have a template anymore, you do not have the biometric template but you simply have a fully random and secure set of signal verification codes. So because we do not store the biometric template we do not have personal identifiable information. It means that it's possible to store that information, to store the verification code, on a card without compromising privacy. And the market that we are targeting today is very much focused on ID-Cards, e-IDs and e-passports. And why is that? Because in many countries e-passports are rolled out, e-IDs are being rolled out, and many of these e-passports and e-IDs are equipped with fingerprints. So if you apply for a passport you have to provide a fingerprint and that fingerprint is stored in the e-passport or in the e-ID. The current protection mechanisms available in the e-passports are extremely complex. In Europe, at least, they are based on what they call "Extended Access Control", that is a system invented by the BSI. And it is so complex and it is also so secure that virtually no one in the world is making use of that fingerprint information in the ID-Cards and in the e-passports. And what we are now doing is, because we are not storing the biometric template for just anonymous verification code, we store that in a location in a chip, in the e-passport, which is not protected by this heavyweight security mechanism. And that means that many more people, the banks, the social services, the government, the police, they can read this document, they can read the anonymous verification code, and they can make sure that the holder of an e-ID, the holder of e-passport is the rightful person. So they can check the anonymous biometric measurement with anonymous biometric measurement on the card, on the e-passport. So they have a very strong authentication of the person.

NBSP: But when they do that authentication it does not provide an identity per se, it simply says that these two match?

Van Der Veen: In that case, yes. So in the case of the ID-Card, it is saying, "Well, this is the rightful owner of this e-passport or this e-card" so it's a verification. Obviously, if you want to use it in an identification mode, that is possible as well. You see, for example, we have a deployment in the payment sector or we have a database, a database of anonymous verification codes and there, you look up an identity in a database. I would say that it's more an application choice than a privacy choice. If a customer, for one reason or the other, requires a card-less system then you go for identification in a database, and if they want to have a card then they go, usually, for a verification system.

NBSP: But in a large database you could come up with an identity of an individual based on what's on the card?

Van Der Veen: No, if you have the... not based on the biometrics, because the templates are not stored in the cards.

NBSP: Okay. But you have something on the card that would allow you to pick that individual out of a database, a large database, for identity purposes, is that true?

Van Der Veen: In what application? I think it's application specific so I'm not sure if you have something in mind.

NBSP: Well, let's take the primitive example of an access control system and all of these identifiers, even though they're not the biometric templates, are in a large database. And an individual comes to a portal and swipes the card, and it matches somebody in the database. Does that tell you who that individual is?

Van Der Veen: It depends how you design it, obviously. So if you have a database and based on this anonymous biometric template you do identification in a database and in the same record, you also place all his personal information then, of course, you know who it is. But if you want to go for a good design, what you will typically would do is you have a separation of purpose, so you would make a purely biometric database with anonymous biometric information, and all the data that is in the database can be used in the access control. So if you would find a match in a database for an access control system, then that person has access to a particular space, for example. And if you design it properly then that will not lead to the identity of the person. But if you want to have the identity you can do that, but that is not a biometric thing but a system design choice, I would say.

NBSP: That's an application thing.

Van Der Veen: Exactly.

NBSP: For example, if it was a nuclear facility and there was an emergency, you would want to know where everyone was, in the plant. And so you would be tracking individuals. And in a theft risk environment, say, you are making diamonds or whatever important things, you would want to know where individuals were throughout the day to track problems that may occur later, and that's an applications issue, isn't it?

Van Der Veen: Yeah. So if there is a valid reason to do so then, obviously, that is possible. Important then, is if you put a biometric data in a database and you also have the identity, make sure that the biometric is fully anonymous, because if that is compromised, yeah, then it's only compromised for that specific application and it cannot be reused or misused for other applications.

NBSP: Would you characterize a BioHash as an anonymous biometric?

Van Der Veen: Yes

NBSP: Well, you used a phrase on your website, something about an enrolment kiosk to register a person, based on fingerprint and their biographical information. Doesn't that imply that somewhere, there is a database with biographical information in it that can be associated with a particular identity?

Van Der Veen: Also, that depends on the application, I would say. So if, in this case of this nuclear power plant, it is required that biographic information is coupled to the anonymous biometric information, then you would do so. If it's, I would say, proportional to the use of that system. If you would do it fully anonymous then you would leave out any biographic information.

NBSP: Yes

Van Der Veen: I think if you look at small access control applications, let's say, for office buildings, and if you look at the proportionality compared to this nuclear power plant, yeah, then I could imagine that a good way forward in that case is not to store any biographic information in the same database, as the biometric database. But that also depends, obviously.

NBSP: Okay. You mentioned on your website, a couple of aspects of the... well, I'll call it Ashara but we're now calling it BioHash, more correctly; the software package, such as administration for editing the database and the ability to operate over network or self-maintain fully online, what sort of data protection would you use when you're operating over networks?

Van Der Veen: Well, there is a little bit of design choice, so the first layer of defense is to make sure that the biometric data that you store is anonymous, so it's based on cryptographic hash functions. That is what we cover, that is what BioHash does. The second layer of defense falls back to standard security mechanisms that you have in every database. If you a database then you encrypt the data and you make sure that you have a key and that you have a proper key distribution, such that only the right people have access to the database, etcetera. And then, of course, if you have communication between different terminals or between the database and a terminal then you need to secure the channel and also, for securing a channel you have standard technology that can do that in a very solid way. So these are all off-the-shelf components that are available and used on many, many locations today.

NBSP: Do you use invertible or non-invertible transforms in your process?

Van Der Veen: Yeah, we use a cryptographic hash function and we use standard components. So if you look on the internet, we use the SHA-256 that is in one-way encryption function. If you input biometric information then the output is fully random, so it's fully encrypted and it's not possible to go back. So we have a non-invertible transform

NBSP: Non invertible, okay.

Van Der Veen: Non invertible, yes.

NBSP: Yes. You know, as a non technical person, I'm always of the question; well, if it's non-invertible, if you can't find biometric information in it, how does the person on the other end know? Is it simply a match and they say, "He is okay to be in that area" or...

Van Der Veen: Yeah, you have to see; the easiest way is to look, again, at this password system on your own computer. If you log on to your computer, you type in a password, and what is happening in the background is that this password is encrypted with a non-invertible transform. And that encrypted password is compared with an encrypted password that is already stored on your system. So the

comparison is done in, you could say, the encrypted domain. And if they are identical then you are granted access to your computer. Now the same thing is happening in the biometric case; so you have, somewhere, a database or a card on which the biometrics is stored, and it is stored with a non-invertible transform, the same cryptographic transform that is used for the passwords.

NBSP: Okay, that makes sense given the variability of a given biometric feature or the way it's presented, does this have an adverse impact on accuracy; false match, false non-match rates?

Van Der Veen: No, it does not, and that is actually the claim-to-fame that we have; that is part of the development that we inherited from Philips. We have about 32-to-40, many years of R&D in it, from the Philips research laboratories. And the key challenge that you need to tackle is to make sure that you remove all the variability that you have in the biometric measurements, because you can have warm fingers, cold fingers, dry fingers, wet fingers, you have different scanners and you need to be robust to that. And that part is all solved and internally, what we do is we have test bench and every week we run our system on ten different public databases, from the FEC, from the MCVT, and we compare our result with the state-of-the-art that is available on the market. And what we've seen on what's possible today is that the matching accuracy, in terms of false accept rates, false reject rates, failure to enroll, is comparable to the state-of-the-art. And in state-of-the-art, for example, if you look at Neurotechnology, that is a vendor which has a pretty algorithm according to the state-of-the-art today, and it matches our operating points; they are in the same ballpark, sometimes we are better, sometimes we are a little bit worse, but on average, it's almost the same.

NBSP: That's great.

NBSP: Okay. Mr. Van Der Veen, I'll tell you what the next steps will be; there are a number of other companies that we are going to have an initial contact with, like we did today. And when we get a better understanding of the different approaches that are being taken, we would very much like to be able to come back to you with some questions that are prompted by what we're learning from other organizations as well. And please don't get me wrong, I'm not trying to pit one technology against another; we're just trying to be able to get a good understanding of what are the best features of each so that that information, we can ultimately provide in our final report.

Van Der Veen: Yeah, perfect

NBSP: Okay, we'll keep you apprised of things that are going on.

Van Der Veen: Great.

NBSP: With that, I thank you very, very much for your time, and I'll look forward to that one brochure that you mentioned, that you might be able to email over to us.

Van Der Veen: I will send that to you. Thank you for the interview.

NBSP: Thank you, very much.

Van Der Veen: I hope I could be of help.

NBSP: Thank you very much, we appreciate it

Appendix “C”: NBSP interview with Dr. Terry Boulton, President and CEO of Securics and Mr. Matthew Ennis, Consultant to Securics

Representing NBSP: Mr. Russell Ryan, Task Manager, Mr. Gerald Williams, Consultant to NBSP, and Mr. Justin Smith, Technical Representative.

Securics Inc.

Securics is a privately held corporation formed in 2004 and headquartered in Colorado Springs, Colorado. Securics was formed to solve a significant problem in non-revocable biometrics: once biometrics are compromised there is no canceling them. For additional information, visit www.securics.com.

NBSP: I appreciate you taking the time with us today, Terry. As I mentioned in the email I sent to you earlier, basically what we’re charged to do under the current BiNS contract is review what’s going on in the major government agencies and departments with respect to biometrics and privacy. And it’s interesting that, at some of the conferences we’ve attended, privacy is looked upon as a sleeping giant as I think it was phrased in one of the sessions last October. Most everyone says that but when we talk to people in government agencies and others we got the impression that “... well no, it’s not really that big of an issue.” In the general forums people talk how important privacy is going to be, but when you try to pin them down they don’t get very specific. To me it’s a question of is it not an issue... or is it really an issue and we just don’t want to talk about it... or is it an issue that they’re unaware of? So we will interview privacy officials in DOD, DHS, and State to assess what, if any, problem biometrics and privacy are causing them now, or what they think may be problems coming down the line. At the same time we’re looking at some of the newer privacy enhancing technologies. The purpose of today’s call is to solicit your thoughts on privacy in general, and then to better understand your technical approach to it.

SECURICS: Okay so let me address the top level privacy question. To me it’s also important to remember that privacy and security in biometrics are actually highly tied. I’ve presented this idea in

multiple talks which I call the biometrics dilemma. And the issue is that with traditional biometrics whatever biometrics database you have is pretty much the same database of those biometrics that other people have. If they have the same people involved this presents a privacy problem because it provides the ability to link across databases and likability is a privacy concern. It provides a security concern because it means that there is a possibility that people using a database outside of your control can get biometrics data that can then be used to attack at a security level what's going on. There are actually two problems. The first of which most is that people dismiss pretty quickly the television type things which is of course making or spoofing data where I can make fake fingerprints or spoof biometric data in some way. And again that's both a security and a privacy concern. It's a security concern if that spoof data is used to violate the security of my facility, it's a privacy concern if that spoof data implicates somebody in a crime or if it's used to wipe out the personal bank account in a way that doesn't impact the organization that owns it because they say well you know that wasn't mine, your fingerprints showed up at the ATM, your bank says that's your withdrawal. That worries people at the personal security level and hence privacy type of concern. So the biometrics dilemma about databases being shared is one of the problems. The whole reason I got into this field actually, is when I heard Arun Ross give a talk a long time ago about "cancelable" biometrics I realized how important this problem is going to become, because the more and more widespread biometrics become the greater the risk that compromise of one person's database could impact the security and privacy of somebody else's database and that's a big part of what I've been trying to solve.

So the other issue in terms of your comment about do people recognize the issues of privacy, I think even end users don't. In another talk which I commonly give in fact in many different ways people don't understand the value of their privacy until they've lost it, until it's been compromised. And if you look at issues related to the use of Personally Identifiable Information and (PII), storing databases and social security numbers for a long time no one thought it was a concern - it was a convenience for various organizations to use that type of identifier to be able to identify people. And then when it started becoming a big problem in terms of identity theft and it actually started impacting people, all of a sudden we had this massive rush to protect this stuff because it's a problem. Now with lots of things like my credit card number I get to cancel it whenever I want. And in fact most credit cards get cancelled on a routine basis just as a security concern so it's a good for a little bit of time and they are automatically cancelled and then they issue a new one. We don't get that with biometrics, so we started out thinking about next level problem, which is online identity. This private security concern becomes much stronger. In the early days of the internet and E-commerce there was a lot of concern about how people would be able to protect their data. Then Public Key Infrastructure (PKI) became important because it allows us to have asymmetric communications between two machines and have some level of certainty with respect to the security of the communication. But we'd only certify the machines, when we need to certify the *people* that take part in transactions. Right now we use ID and password as a dominant thing and the phishing that goes on is rampant and it's growing in sophistication ... it used to be if I was careful with my browser or whatever I was pretty sure I didn't go to bad website.

Now with things like man-in-the-middle browser attacks, there are ways that PKI just can't protect the machine the way it used to and PKI was never designed to follow identity issues. So a big piece of what we want to be able to solve is maybe using biometrics for verified and here I say "web identity" because in the future I think that's a big piece of what we're going to be able to deal with. It's not just verified identity when I'm standing in front of a person, but verified identity through the network. And that's, I think, the place when biometrics really starting showing a lot of their added privacy concerns because if my biometrics data is hacked, or phished, what's going to happen with it? How do I convince somebody the computer on the other end that happens to have the biometric isn't sharing with some other random person in a different way? There's a lot of added issues that come up when all of the sudden it's an anonymous person on the other side of the internet connection that I can really can't verify ... how do I make sure who they are? We can't just try and match biometrics in encrypted form because I can't mess with them when they're encrypted so I have to decrypt them and a lot like symmetric encryption that we use to have before PKI, both sides need the keys for biometrics. Both sides the matcher and the matchee have some level of biometrics. They have to share some symmetric key for encryption and then you have to worry about what happens if the other side gets it. And if you think about it from the security point of view and not a privacy point of view no one who is really serious about security would use accounts or tokens or passwords that couldn't be revoked. And the security question is why we accept less from biometrics solutions. And a piece of where we're trying to take this is to be able to move to that model.

I introduced this idea of the fallacy of secrecy meaning that there are lots of people who from a security/privacy point of view say that biometrics cannot be secret because we can leave them lying around or whatever therefore they don't really need to be protected. But credit card numbers aren't secret but they have to be protected by law and it's really not about whether or not it's a secret about how the information could be misused, how it might be abused and therefore whether or not requires protection. And in my view, the real risk of biometrics is not the fact that we might leave a latent fingerprint lying around here and there. Sooner or later when you build a big enough database it will have enough value as the risk in value of that data changes to make it a worthwhile for somebody trying to attack it. If we can build something where the database has much less value we increase the security of the database because there is much less reason to want to hack into it. As we make that value go down and down the value equation changes.

The doppelganger attack, in my view, is one of the biggest risks we have and one of the ones I was most concerned about in the sense that if I have a big searchable database of 6 million people in DC and I'm looking at a system that uses biometrics and its false accept rate is running at 1 in 10,000, how many people in that database accidentally match my fingerprint? Now you can say one in 10,000 is not accurate enough, I'll run at one in a million that's still a non-zero chance of finding somebody who I can have what Jim Wayman calls a zero-effort spoof attack. I put my finger down and it's accepted - at least with high probability - as that person. That kind of a problem is a big issue when we get to stored databases that can be searched because it means if some Gym has a very large searchable database and somebody can find out whose fingerprints they're an acceptable replacement for, then they now have

an identity whose biometrics is at least at some level a replaceable item with that person's identity. Now was there a question there?

NBSP: Doppelganger is close enough, is that the application?

SECURICS: Yes, doppelganger is close enough, and if I had a large database that I can search through then I can start trying to automate the search for a doppelganger. And if I find somebody who is a body double, stand-in double for whatever biometric you want ... that presents both a privacy concern and a security concern because this person's identify is now at significant risk and once that happens, once I know that I can match somebody in a database it's very hard to take that back. So again it comes down to a lot of the issues are trying to deal with how do we protect the database, how do we protect that stored data. This is a national biometric challenge, this is a recognized national need, although the idea of a biometric template that can be revoked is not something that is getting a lot of attention, but obviously you guys are looking at the alternatives that are out there.

So a little bit about my history and stuff. I've been actually working on this since around 2000 when I first heard Arun talk about it, but I started publishing on it around 2006 when I finally came up with a solution. We take whatever biometric you have, we take some other key information like a company ID and a company key that makes it specific to a particular database for a particular company. We take a user specific public key and we can take an optional password, we don't have to have a password but if we do it will have a secondary concern on privacy. So when we do all this there is a mixing which I'll talk about more a little bit that produces what we call a "biotope". And the biotope requires that all of these factors come together simultaneously: the biometric data, the company ID and key, the user public key and the user password. Now the company ID and the user public key, all that could be public or the company key could be private to a company that they never published but obviously they have it in their system so they can always use it. So the only two things that are sort of semi private here are the users biometric and then if the user uses it, the password. Now the password can be important because it means two things, the user has control over the data. From a privacy point of view this means they know nobody can use this data without my password and if I protect my password and my biometric, now I have an increased model of security, two factor authentications commonly considered for that. An important difference is we don't store the factors separately they are stored together. So you can't get one without the other. Traditional two factors store the biometric and the password separately. A second important thing that's shown on this slide for our technology is that once we have one of these tokens we can derive a new token from it and derive another token from that and as we do that we can not only derive new tokens, we can embed new keys inside of that for each transactions.

NBSP: The company ID and the key - explain what that is, is that like a digital key, is it similar to a PK, a public key or what is it comprised of?

SECURICS: So the company id and the company key, we actually separate them so that we actually store the company key associated with the biotope so that if we find one later we can know whose it is, but we never store the company key. So we have sort of a licensed key in one level if you want to think of it

that way, but this is something that obviously the company would have and in our case it's just a number, it's some random number that the company has it's not a public key. The user public key actually is a public key and the user public key is something we use because our technology allows you when necessary to revert from the stored token back to the original data. And I believe that's actually really important, so I'll talk to it now. In the sense that if I have a transform, a non-invertible transform like IBM talks about or the type of fuzzy extractor stuff that PrivID people does. If you build a revocable token but the only way to revoke it is to ask the user to come back in and re-enroll, then the company or organization behind that revocable token is very, very unlikely to ever want to revoke it because the cost of revoking it is extremely high. So our technology was designed from the very beginning to allow us use this public key technology and multiple other stage processes where the system can go back from one level to the level before it by using the appropriate private key. And in the case of the user public key when you enroll you give the user their private key for them to protect and if they have it then they can re-enroll in the system without physically going anywhere because they can take their old token, derive new data and then move it forward and reuse it. Now in our case because of these derived keys which I'll explain a bit more in a second - with the derived keys most of the time you would never even go back to the end user. You would re-derive keys from the intermediate keys and I'll explain how that happens, but this idea of making and revoking the token in fact virtually free is critical if you really want to have a truly revocable token because would you say, okay, well we've got the database that has 2 million customers *might* have been hacked. We might've had a security compromise, so everyone come in and cancel it. And so it's sort of like your social security number, you don't cancel it unless you're very sure it has really been used you can't recover it and clean it back up because it's too much of a hassle. But it's still much more cancelable than something that would require people to specifically come in and re-enroll the fingerprints and everything. So that's why we have the user public key. The company keys are just so that every database for every company is non-exchangeable. Without the same company key, the data you're going to get isn't going to be useful at all. Does that answer your question?

NBSP: Yes, thanks.

SECURICS: For the finger biotope we take your biometric fingerprint data and we extract features, in this case right now all we're using is standard XY data - minutia type information. From those we actually use a variation of the pair type table that is used in the Bozorth algorithm. We mix in all the keys and we generate a token. And the important thing is once we store that token in encoded space we never have to decode it to match. When a new token comes in we can match the two in encoded space. And in our papers we do a security analysis of this and for a Brute Force attack for somebody who knows all of the keys except for the user's private key which we never store and we don't actually have a need. The attack takes around two to the hundredth operations and for somebody without access to all the keys it takes about two to the 120th ... if it's possible at all. There's one-step we don't know how to do, so we haven't been able to attack it. We just assume that step is free because we don't know how hard it really is which is standard in the crypto world ... if you don't know it assume it's free. There are actually 13 dimensional structures and we're projecting them down in the space where position and color are

affected by the token. When you change those keys you get a radically different change in the underlying representation. So once you're in the same key space in fact if everybody uses the same key then you're pretty much to a traditional biometric problem, but as soon as you change keys the two databases are not at all interchangeable and you can't look somebody up using one and the other.

NBSP: So you now can create multiple keys from the same biometric?

SECURICS: We do not extract the keys from the biometrics, the keys in our case are external data that's provided, so I might have a company having two keys, I might have one key for the user like their user ID and then the company key if I have a two level key. As you'll see in the second we can have trees and then in the trees and we have more keys. We can add as many keys as we want along the process. But the keys are not extracted; the keys are external data that sort of says this is the set of transforms to use for this person's biometric. They affect what transforms would apply.

NBSP: And just quickly would you then use different keys to access different types of database, in other words in individuals financial data maybe one is medical and maybe another?

SECURICS: Yes absolutely that is the point. For every application, and as we get further on eventually for every transaction you do, there will be a different set of keys so that you never reuse the token a second time but yes the bank would be different from shopping and other applications. So in the next slide the sort of secret underlying our approach in the biggest differentiation for our technology from a lot of other people is when I was trying to solve this problem and I tried lots of various techniques early on, there were two very different things I wanted. I needed something that had a robust distance in matching property because biometrics require the sort of robust distance in matching and at the same time I wanted security and revocability and every technique I tried would either give up too much on one or the other. And eventually I came up with this idea that I had two different goals so maybe I would break the data up into two different parts. So in our transform, we take features and we actually use things like distances and angles and whatever. Let's use height as an example - a very rough idea. So you can think if somebody's height is being a stable part which is their true height and then they are unstable part which might be my measurement error or might be the fact that they were in shoes that day and I can't tell, it might be that their spine compresses or whatever it is, there's some stable part of their measurement and an unstable part of a biometric. And I'm going to break a data up into those stable parts and the unstable parts. And the important observation is that the stable part is by definition stable and once its stable I can encrypt it, I can hash it I can do whatever I want to protect the security and privacy of the data and provide revocability. So if I take that stable number, I append on some other number and I then public key encrypt it, I get something that's revocable because I can change the stuff I appended to it, its invertible with the public key as long as I have a private key and yet given the data nobody can get to what was the underlying space because there was too much ambiguity. And now I have the unstable part which has actually been transformed so it's somewhat privacy protected but the unstable part has all of the other remaining unstable bits and I can combine the two together and in our papers we prove that if we started with a windowed robust distance measure then after this transform you can prove it doesn't decrease your accuracy because the stable

part is still there and all those been transformed you match it exactly anyhow but then you just add in the areas from the unstable part. And this is really what makes biotokens work is, we've kept the security part, the stability, and the accuracy part to the unstable data that's now privacy enhanced. So if you think of it as a windowed operator it doesn't really matter where we draw the window, there are really two functions we need to know. Are you close enough to the data for us to bother measuring errors, and if you are then we use a least squares error, which is commonly used. And if you're outside of this window we don't care, we just know you're outside so we give you some confidence penalty. And this allows us to use this sort of modulus-like computation to protect things and still keep all the distance measures together. So now that went by pretty quick do you have any questions on this because this is really fundamental to what makes our technology simultaneously accurate and secure because we get to encrypt the stable part but use the unstable part as part of our distance measures.

NBSP: Just to make sure I understand, the window effect is taking this first look at it and seeing whether its close enough even be measured?

SECURICS: Right. If you think of the stable part so let's say, again going back to the height example I said that I can accurately measure height and my stable part is plus or minus 6 inches. So I can define a window size the sort of window would be 6 inches and I can center the window anywhere I want but then given that I'm not going to tell you exactly which window you're in so I could make the windows show up on every zero and 6 inch boundary and then I could tell you that somebody's height is windows 7358 which is after encryption some window plus two inches. Well that I haven't told you much about the person's real height because you don't really know where exactly the window was centered, that's a person's specific thing and you don't know anything except that within that window they are two inches from the boundary, but you don't know where that boundary is so we haven't revealed much about your information and at the same time you can still get all of the accuracy and well if this person is normally in this window and I've instead measured 4 instead of two you can decide how much a penalty you want to apply because you're two inches off in your measurement. We took the original NIST Bozorth algorithm and just changed small bits of code to make it work as a biotope algorithm and in this case we're showing how, not only did we not lose accuracy in fact we gained accuracy. And the reason we gain accuracy has to do with the initial lifting we're doing and the fact that there is a little bit of random transform for everybody. As I said, these windows are person specific they depend on transform and when we go to do that if somebody is close to you and they follow you exactly then they'll have the same distance they did before but since everybody has a little bit of random transform stuff going on somebody who uses a different transform that might have been close to you initially might end up with a different enough transform that you get separated. And so we get a little bit of dimensional lifting out of this. It's not much, what it really means is that the Bozorth algorithm left information on the table. If they had actually done a really good job of eking out all the possible information we wouldn't have been able to gain anything but in this case we were able to improve accuracy. And for privacy enhanced technology this is still the best reported accuracy on public databases that has been published. And to me that's a really important issue if I get a revocable token but I have to give up half my accuracy and I get a system that has a false reject rate of 90% at a

reasonable false accept rate no one is going to want to use the system. So it doesn't really matter that I protected your privacy if no one will use it. And then from the security point of view if I don't maintain accuracy then I impact security and those are two important tradeoffs. Let me describe the idea of what we call the biotopes multi ID. There's lots of different ways of looking at it and I'll explain more in a second, but one of the things that becomes very important I think, it actually goes back to one of the reasons why I was interested in trying to talk to you guys before, because at one point you're trying to build this large database to solve the Anonymous Biometric problem. In that sense biotopes offer a really interesting proposition which is if I build a strong root ID for every person and I do deduplication and I know for sure the loss for any proofing and I know who this biometric is. From that one very strong ID I don't have to actually use that ID except for deduplication against other IDs. I can take that root ID and I can generate an ID for their bank, I can generate one for working, I can generate one for voting and each of those tokens is derived from the strong ID but they are not interchangeable and any one of them is revocable. This becomes an ideal for web based identities because I could make them so that they can be cancelled whenever I wanted, I don't have to worry about them being phished or stolen.

NBSP: Is this a similar principle to what PrivID is trying to do?

SECURICS: Not at all. The underlying objective is to have a privacy enhanced token that is revocable and in their case you can't get back to the original data no matter what you do. We share that goal of trying to have this token that I can revoke and it's not traceable back to me but it's very different in the sense that ours allows you to derive new tokens from it that's not something you can do with their technology at all, and I believe that deriving new tokens is critical because otherwise you'll never revoke them. If I've generated one of them but every time I want to go generate a new one and we have to go reenroll no one is going to want to do that very often. For a passport their model might work - my passport is a physical document and if I generate a different token every time I get a new document there could be some value with that but it doesn't solve then the issue here of building one ID that I can do a strong identity proofing over and then after that deriving new ones from it any time I need. That's unique to our approach and it's actually one of the things as I started out I knew how important that was going to be. So I started trying to design things to it. Not only did I want privacy enhanced, in my view it had to be something that I could eventually make transactions specific, transactions unique because if I really want to protect privacy it's not *just* about revocability. In the long run there are some other things besides the fact that somebody might be able to retrieve my data. I've already mentioned in privacy this idea of likability, so the ability to link two transactions over time is another privacy concern and "observe ability" is another one. If every time I use my (and I'll use the PrivID since you brought them up), a PrivID token, if it's always the same token in every transaction then it doesn't really matter that I don't have my fingerprint there it means that my token is trackable and therefore you get all the private implications of likability over every one of these observations. If on every transaction I'd give you a different token and even if you observe all the transactions, you can't necessarily decide who it is because every transaction is different. So what we want here something where the client can make a request for the transaction, on the server side they generate this bipartite biotoken that is unique to this

transaction and send it across, and in this case on the client side we're going to match with that token and we're going to release some data that lets us on the client side prove that the match happened, and then use that key for either cryptography, or authentication token or send it back to the server so the server can prove that the client did the matching. There are lots of variations what we can do with this, but the two important things are it will be unique for a transaction and what the transaction does is not just send a biometric or a revocable token to match, it embeds a onetime use token inside of it so when it matches, both sides get proof that the confirmation actually happened. I want to introduce one more thing before I get there. The biotoken key infrastructure comes back to the root ID, the biotoken we introduced before and this can be very strong and if it's done right this one can be done in such a way that it can be searchable so you can do deduplication on enrollment, or wherever. And now, as soon as it's searchable, it better be a well protected database. From that database I can derive new tokens and one of the things I can do with that token is the token can include a password. So I mentioned before this idea of having a password or non-password. Well if I include a password then everything that derives from that token has to use the same password. But that's okay when I share the password I can remember all of them but every token is still unique. So we have a root ID and from it we can talk about what we call root signed master IDs which is one per application and then each of those can work on down and if you're familiar with way the biometric public key infrastructure works you have this idea of pure signed operators who can issue certificates and they can issue certificates that allow other people to do certificates and there is actually a tree structure associated with that that allows you to figure out how to go back and check, is this valid, has it been revoked and whatever. And with our bio token key infrastructure we can actually build the same type of tree structure in fact we can build it on top of X509 version 3 certificates so that it's actually a certificate that includes one of these revocable biotokens with it and they can talk about who signed it. So for example in our campus project that we're doing for alcohol verification, the person who is verifying the person's age is signing with their biotope that I'm the one who did this so we have a strong non-repudiation – "... no you issued this ID, your finger print was there when this happened." And so this idea allows us to go a little bit farther. But one of the things that's important about this when we talk about transactions and it's not as good, you don't see the way I presented it before. But because of this biotope key infrastructure if Alice wants to find Bob and send Bob a message Alice can have access to this public biometric key infrastructure with say the tiered BCA token for Bob in a public directory and she can say okay, I've got Bob's public directory now, I'm going to initiate a transaction with Bob. I don't have Bob's biometrics but I have Bob's biotope. With that I'm going to use that in the next transaction and when I send it to Bob, only Bob's biometrics are going to be able to reveal the content of the message. So when he sends it back to Alice, Alice knows that Bob's biometric showed up to take part in the transactions and therefore she had a lot more confidence in what's going on. Going back to where I started, this is about verifying the individual taking part in the transaction at a level that is an individual-to-individual thing not a machine-to-machine thing. So with that as a background we can now go back and we'll go through the biopartite or biotope process in a little bit more. So the biometric key infrastructure, both what we're doing with the tree and the idea of individual-to-individual transactions, does that make sense, was it clear?

NBSP: I understand that ... as opposed to machine verification.

SECURICS: I can use the PayPal as example here it's really much the same. The side that wants to do verification, and it doesn't really matter which side starts, sends an authorization request to somebody who has access to one of these base tokens. It doesn't have to be the root as long as it's a viable base. The server side will now take that base token, a transaction ID, and then they can choose some nonce of the key or they can in the PayPal case pull out a PayPal PA key which stores the information about the financial transaction or whatever it is we're going to take the biotope base, the transaction id and this nonce or this key that we want to embed and we're going to use those three to derive a new transaction-specific bipartite biotope. We send back to the remote matcher the transaction ID and then the bipartite biotope and they can combine the transaction ID, the bipartite biotope and now a locally captured biometric piece of data to generate a token that they match against the one they received and during the matching process it extracts a nonce. The matching process inside of it has a little bit of a fuzzy vault-like process and we published some papers on security concerns and problems with the fuzzy vault, but our technique solves all those problems. (That's actually why we knew the problems existed, because we were solving them.) And so when you match parts of your biometric match little pieces at a time to allow it to not just say it matched, but to reconstruct the key that was embedded. And so while we don't derive keys from biometrics, we can hide keys in biometrics and then extract them later which is a part of how we can do some of these asymmetry because now once the remote side has matched they can send back the nonce or the key that they have extracted, back to the server and now both sides actually know the match happened. And this is important at two very different levels. One if I'm thinking about some sort of remote, through-the-web authentication or any type of remote authentication there is always a question of who is trusting who for the match. In one case the remote side sends the data off to the server, the server does whatever it wants to match and then sends back to the remote site, "yes it matched". Well if there's somebody in the middle who could fake the yes it matched message, the remote side actually has no idea. On the flip side if you let the remote side match the server has the same problem they send data of to the server and say it matched. How does the server know for sure? In our case the server generated the nonce the remote person can extract it and as soon they can do that they know that the other side really had the real data because if the server didn't have my real finger print they couldn't build me a biotope that when I match actually extracts the nonce. So because the match process knows that it was valid so both sides actually have confirmation now that the other side has the data they say they have. This is now how we moved from machine level of identity to person because both people know the other person has the appropriate piece of data. You can take it a bit farther and actually run the process both ways with bipartite biotopes going between two people to ensure that this happens. You can actually use this to do a full digital signature with bipartite biotopes for both people. This solves the asymmetry matching which I just went through. You know it's also really important for solving man-in-the middle, and phishing attacks because even if somebody were to capture all of the data being transmitted and assuming its transmitted with no encryption, it doesn't really matter because the bipartite biotope is single use that has no replay value. It's not revertible back to your biometric and it's not matchable across two different transactions so there is not any information obtained by somebody who gets that. In terms of having a remote device being hacked if I'm the remote side I can actually do this is such a way that I never ever send my fingerprint anywhere. The server is sending down to my PC the bipartite token and it doesn't matter

there is no man-in-the middle that can actually capture that data it will be unique for transaction and so I don't have to worry that my data is going anywhere, its staying in my local machine. And although I've described this as a real time transaction, all of this can be done completely asynchronously sort of offline with synchronization or I can use this to store an encryption key that I stick on a USB stick because when the bipartite biotope gets generated and when I match, it doesn't have to be in real time, it's an asynchronous protocol. So does this make sense? Any questions on this piece?

NBSP: No I understand what you're saying.

SECURICS: As I said, one of the things we're worried about is making sure we have accuracy and for these bipartite things we have to make sure we can store keys of interesting sizes or it's not going to be very interesting. So the closest related work is a fingerprint fuzzy vault work out of Anil Jain's group, in terms of embedding data. The PrivID work is okay but they have no published results on accuracy so we can't compare them and they can't hide keys so we can't compare on that dimension either. So Jain's work was getting ..., with false accept rates around 10% ... they were getting true accept rates around 90% when they are embedded about 100 bits, 120 bits of data. And at these small data rates the data sets are too small for us to get any false accepts and we're getting 97% true accept rates. So very high rates and this is on FDC type data. We then looked at what happens when we try and install larger and larger amounts of data and our system has a couple of parameters like error correcting bits and whatever. As we get to storing larger and larger keys, a 512 bit RSA key is a pretty big key we're still in the high 90s true accept rates for our data. We also looked at when you get starting using these larger keys, certain fingers (because if you don't put your finger downright you just don't have enough information). So we did some experiments looking at what happens if I try multiple recovery attempts using basically the FDC data that has 8 prints per person we used one per enrollment and that we just started saying well treat each of the others as an attempt. And you'll see that after 5 or 6 attempts even with a 512-bit key, we get 99% true accept rate after 4 or 5 attempts. So we're getting very high true accept rates. Now when we look at the false accept rates again the FDC data sets, because they only have 800 images, are just small to be interesting for testing the newer version of our system so we developed what we consider doppelganger attack tests. We built a large imposter set using every fingerprint image we could get from every publicly available database we could get our hands on and using the 512 bit tokens and 128, 216 and 512 tokens we have zero false accepts in over a billion imposter trials. So for each one of those we went out and tried a billion false matches and we're still getting zero. Doesn't mean zero false accepts, it just means it's smaller than one in a billion that's about as far as we could test. The balance between security and privacy has got to be considered if we want to look at large scale utilization. The detail for these experimentations, and you have to look at them carefully to know everything that was going on, but we feel now confident enough and this was now secure enough and accurate enough that we could begin trying to collect it.

One of the things we're doing with that now are PayPal transactions. We have an approved application from PayPal for doing 3 different operations. The first is fund transfer, the second is shopping and the

third is merchant or bill pay and I'm just going to walk through on the next slide how we do one of those transactions which is the sort of shopping transaction. So in the shopping transaction the sender goes to look up whoever they want to enable to shop – themselves, or say a parent wanted to enable a child to shop while at college - they go look up in the BKI DB the person they wanted to allow to shop. The sender then logs into PayPal and when they actually log into PayPal they catch what's called the PA key, this is the number that if you have this number and you can charge against the person's PayPal account up to a certain limit. So that number has to be very well protected because it's the equivalent of cash from PayPal. We take that PA key and now we embed that inside the bipartite biotope with the transaction ID and we store that in the database. Then we can send mail to the merchant so the merchant knows when the user comes in, the merchant can say "... Oh, this user wants to use PayPal," then go click on the email and verify whatever they want about their merchant process. And then basically the shopper puts a fingerprint down and when they do, it releases the PA key and the merchant's software automatically takes that PA key and transfers money from the sender's account to the merchant's account and you get the money. What we're doing is using the biotope not just to authenticate the user, but actually to add the support and storage mechanism for the PA key that has to be protected. Any questions on that kind of process?

NBSP: If I'm understanding all this correctly, some approaches have been to separate the biometric and PII, but Securic's approach is to combine the biometric with other data into a bipartite biotoken, or biotope as a means of protecting everything in the database, PII or not?

SECURICS: Yes because now every database is not matchable so there is no linkability across the databases and if they are revocable then if the data gets revoked you can cancel it so it protects PII in the sense that if I were to have it in my database, my database gets compromised nobody else's data is impacted in any way. I cancel mine, I revoke them all and I reissue my tokens to my customers and I don't have to worry about anybody else's. And again if you go back to the tree thing that I had introduced earlier, one of the things we recommend is in fact that every application has its own root, so there is a root which is the one you get strong ID with. And then every application has its own master and I never use the master in a day-to-day operation I take my master and put it off on the side, so that when I want to cancel and reissue I just take my master and derive new ones from it which is easy to do. And then I never have to bother the customer to go back and say I need to reissue you a new one. It's just like you know this month your operational token is changing you don't even know it because if the master has your password then every derived one uses the same password and I don't really know what the password is. So I never store your password. When it's in the system this way once it's stored, its stored and there not two separate factors to be hacked separately.

NBSP: Got it, I understand.

SECURICS: Underlying windows log-in and almost every single sign-on tool is a protocol called Kerberos and as it turns out it's a well known fact that Kerberos is itself subject to a security attack in the sense that password guessing is not solved by Kerberos. So it doesn't really matter if I use passwords because if somebody watches that transaction and captures the messages that are used they can launch a

dictionary attack against that. And in fact many biometric implementations of log-in use the biometric to release a password, that then uses Kerberos because it simplifies integration with Windows and that means that they are still subject to the dictionary attack because it all depends on releasing the standard dictionary password the person had. We developed a version of this which we call Bio-Kerberos that uses our ability to transmit stuff in such a way that its immune to that dictionary attack because the tokens are different in every transaction and we never use a standard password. Integrating that with windows was a pain so we developed the idea of what we call Orthros or a bipartite log-in where we do the same thing except we use the ability to transport data to basically transport a one time password. When a user wants to log in the system generates a one time password, updates the Microsoft database, embeds that password in a bipartite biotope, and sends it off to the client. When it matches, the client gets the one time password that gets used to log them in and then the password is changed again. So that it doesn't matter if somebody compromises all of the communications it's a onetime use password. In fact it's very similar to the way that an RSA secure id interface would work and in fact the number we store in it could be a RFA secure id token and now you can use it if you have a token you use your RFA token if not you can use your finger prints in place of it and you can build an infrastructure that does all of this.

Let me explain a little bit of competitive differentiation of the key features of what we're looking at compared to some of the other things out there. GenKey for example, I don't know if you guys were looking at them but they have an unknown model of accuracy and unknown model of security because they don't publish that much of what they've done. And to revoke and reissue requires physical enrollment.

PrivID is better even though they had no public accuracy, the model of how they are securing the data are well enough understood that I'm reasonably conformable with most of the security. The one concern that I have and the reason I have the privacy checked is they are linkable, so you can watch them across many transactions and everything is always the same token. So they're highly linkable and in their process they have a bunch of helper data and they've never published what their helper data is. So it's very hard to know what information is leaked because of the helper data. In the extreme if that helper data was raw biometric data that allows me to say well I expect these minutia to be in the following small windows and they have this type of minutia in this window and this type of minutia in that window, I may not have leaked completely what their finger print is, but it may have leaked a lot of information. So because I don't know exactly what they are doing on one part I can't pass judgment. I'm not saying it's not, it's just not been publicly announced what it is, there is some concern there. IBM's cancelable techniques, at least the version they've published a year ago, still have security flaws that we've already told them about. We published one or two of them publicly we told IBM about some of the other ones and their accuracy is somewhat fair. It's hard to say because they only tested it on internal IBM databases they never publish results on publicly available databases so it's hard to know where they really stand on that. Their technique has lots of interesting potential, but until they resolve some of those security flaws and the most obvious one if you've looked at their technique is that they basically perturb the image in such a way the minutia get perturbed a little bit, and in their paper from

two years ago, their folding technique is mathematically not invertible but only about 8% of the data has any level of ambiguity when they get done. And a fingerprint matcher will gladly accept if I had 8% garbage data so if I take the 2 point ambiguity that gets introduced by their data and I just take points that say well I can't tell if it came from A or B but I'll make a data that has both A and B and I build a massive thing when I invert it, a fingerprint matcher will still match it because it doesn't care about 8% noisy points being added. So that's one of the security flaws that we've already told them about they're trying to work on fixing it. And then the other standard stuff is sort of well known. So coming back to this from the privacy point of view, what happens when your data is lost or stolen that's a concern and obviously with biotopes we can revoke it and reissue, we can even generate them per transaction store them on a smart card server and never reuse them which goes a bit farther than the traditional idea of well, how often can I change it, it's a onetime password that never gets reused.

If people are worried about privacy and function creep and if we use biotopes with a user control password, without which we can't generate your biotope, that level of control addresses a lot of people's concerns that this could use for things without them knowing it. In fact one of the tenants of privacy is often that the user has control over when and how their information gets used and by having something we never store such as a password we give the end user that model that can happen. Understanding that in certain government programs you have a need to balance revocability and non-repudiation just because it's revocable, just because it has the user password doesn't mean you can't trace it back to the user in the right process. So if we have this idea of a master database with a root id we can prove when a token is derived from a base token even if we don't know the password, but given just the password protective version we could never search for the user. So these databases with this model going back to our start in doppelganger problem is now a non-searchable database or it's searchable only in the sense that if I get the users fingerprints and passwords simultaneously I can search it. So the user can imputed their fingerprint and a pin and then search a database to find them that's fine, but I've made it much, much harder to search because now I have to guess the person's password, so it's made searching impractical for an attacker to try and easily find doppelgangers which is both improving security and privacy. In terms of traditional biometrics it is a question of how do you ensure the match exactly happened, is it really happening because you normally just get a yes or no type answer and with ours we support this embedded key which allows you to know for sure this really happened. And if you're looking at this from a non-repudiation point of view now you can actually log all these keys and keep track and if it's done with the right set of keys then you can prove that this log message can only have occurred if this user's fingerprint and this machine generated the following tokens. And so you get the non-repudiation of both sides that the base computers keys were used to generate it the end users fingerprints were used to match it, and both sides get a record of what actually happened in an audit trail. And then finally, if people are worried about the government or police using normal databases to search for them the current implementation doesn't really solve that problem because if we use the password version it's fine but if the government has an implementation that's searchable for deduplication we don't quite solve that problem but we solve a little bit of it in the sense that the tokens that they could derive from that can't be used for anything else. So there is a reduced

concern but it doesn't completely eliminate it. Trying to solve the problem of deduplication with both privacy and security is work that we will hopefully publish next year.

NBSP: This is released commercially now, isn't it Terry?

SECURICS: Yes. In fact if you go to epaynotory.com you can sign up and do PayPal transactions.

NBSP: What are the key markets that you're going after? Is it the commercial market, the government market?

SECURICS: Commercial market in terms of financial transactions is a place where I think this becomes a very natural thing to want to use. We believe it has from a market point of view, potential for various government programs again both from the security and privacy model, but if we can get a large scale deduplication program to say I've done where I need to with traditional biometrics to do deduplication but now we're going to issue individuals a revocable token for daily use and then the government can reissue another one later so that we can solve a lot of the security and privacy concerns for a large scale government program in other countries because we don't have one of those kinds of programs here. But we are going after those

NBSP: Can I ask a question about the PayPal? Terry Boulton, I think you said a few moments ago that one customer could go to epaynotory.com and participate in a system. Does that mean that person would have to get a tablet, a fingerprint reader at their terminal?

SECURICS: Yeah. Currently the deployed version only supports the Digital Persona sensor because it's the only commercially available sensor that provides encryption over the USB bus, which is another potential security direction. We're going to release a newer version later this summer that will support three different sensors, but yeah. It's beholden on the user, the customer to have a device. In what we're doing for our university project in a local thing. The person who is using it for shopping doesn't have to have one at home, they can be enrolled at the university desk and then that can be used at other university facilities for them to be able to pay for things. So it's more the merchant who is going to accept money has an incentive to want to have a sensor. People having at home if I want to verify transactions between or if I want to receive money from some family members you could want to have your own sensor at home but that market we expect will be a little bit smaller. Even though we can do certain things in PayPal one of the things we wanted to be able to do which we have a design for but can't deploy, is to verify a seller on eBay or whatever, the sort of seller involved in a PayPal transaction. The problem is the PayPal API does not support those kinds of functions and we've requested those kinds of functionality to be added, but who knows what kind of new functions get added. And so right now it's only the receiver of money that needs to verify or can effectively verify in the transaction and in that processes you'd imagine most of the time it will be the merchant that will have these things.

SECURICS: Did this help? Do you have a better understanding now?

NBSP: Yes. It was quite thorough.

SECURICS: An important thing going is for many people there is this issue they think that they have to give up security and a bunch of other functionality to actually get the privacy stuff. So if they think they have to give up something to get privacy then there is going to be a lot less interest in doing stuff. If what they see is that they can simultaneously enhance privacy and security which is a lot of what we spent our time trying to figure out, it's not like we just have this like one thing which just solves everything. We designed it and used the elements of the toolbox in terms of what biotopes can do in different ways to address their privacy concerns and their security concerns in a way that balance both. You don't have to trade off one against the other, you can possibly improve both of them and I think it's been a big thing of what I try to get across in my talks is that people still very often their reaction is no, no, no privacy is not an issue that my problem doesn't have these concerns and some of that may be their instinct as well I don't want I need this function. If they can say that we need the following functionality then we can say how we can still balance privacy as best we can give those requirements. When we started this process the idea of having a revocable token that would be a lead for transaction for not obvious and though it's not directly tied to this then either we could do deduplication and maintain privacy seemed completely odd but next year we'll publish a paper on how we do that. So the range of problems they have to tell us what those problems are ... then we can go back in and design a solution that combines the elements of what we can do to solve that problem.

One of the things that may not have come clear is that the tools, the biotope and the components, can be applied to different modalities as well. That was an example set using the fingerprint, but there's work going on right now to apply a biotope to voice, and to face and palm, and on a different level in iris, so it's not tied to fingerprint even though that's the platform that most of the demonstration work has been done on.

NBSP: That's a good point. Okay, Terry thanks you very much. I really appreciate it and we will be following up and as we move forward with the interviews as I said, it will probably prompt some more questions but once they get completed and we have access to it, we'll be happy to share that with you and hopefully it will provide you with some valuable input as well.

SECURICS: Okay, thanks a lot.

Appendix "D": Matrix of PET's



PET Matrix.xlsx

