PRIVACY IMPLICATIONS OF BIOMETRIC DATA

Kevin Nevias – CISSP, CEH, CHFI, CISA, CISM, CRISC, CGEIT, CCNA, G2700
09/20/16
What are the benefits of using Biometric Authentication?

ATM Example: Fraud Prevention

Financial institutions have suffered huge losses as the result of ATM fraud. In several instances losses of 15 to 45 million dollars occurred within hours.

Moving from stripe to chip technology will help, but this does not eliminate the risks.

Biometrics significantly reduces the risk, but the added security also brings along significant privacy concerns.
Example of Benefits – Banking in Africa

• Identity theft in South Africa has motivated banks to rethink the way they authenticate customers.
• Capitec - from the initial launch of its branches incorporated biometrics as part of the account opening process with fingerprint scanners and webcam photographs of customers. Other South African banks have followed suit - Barclays Africa customers now provide their signature using a digital Wacom tablet that digitally stores their signature.

Some of the benefits realized

• **Security** - Identification document fraud in South Africa is high as criminals use counterfeit drivers’ licenses and birth certificates to commit identity fraud. Biometric fingerprint scanners can detect and prevent fraud at the point of sale.
• **Safety** - The use of biometric identification protects customers against fraud as once in the system, biometric data allows customers to transact at the bank branch without identification documents which reduces the risk of potential theft or loss of valuable documents.
• **Ease of use** - Biometric systems make it easier for customers in that they require less documentation and don’t require users to memorize passwords or carry tokens.
• **Speed** - Customer experience can be enhanced as banks are able to identify and verify customers quicker and Biometrics can also streamline the application process, reducing the number of documents individuals must provide.
On Device versus Off Device Storage of Biometric Data

The primary focus of this discussion is Off Device/Server Side Storage

On Device Storage (device side)

Example: iOS Touch ID
- Generally used as a replacement for a password/passcode on a mobile device
- Biometric data is not stored or transmitted to a vendor (i.e. Apple, Bank of America, Chase, PNC, etc.)
- User has control of how and if feature is used
- Limited privacy concerns
- Will this data be stored in the cloud in the future? Probably – Apple already has patents for this capability (although we have no way of knowing when or if this will be enabled).

Off Device Storage (server side)

Examples:
- USAA: (fingerprint, voice, facial), MasterCard: (selfie-pay), Diebold / Citibank
- ATM (pilot): Iris scanning, DMV (facial)
- Generally used as a replacement for a password/passcode on mobile/non-mobile device (i.e. ATM, phone, etc.)
- Biometric data is stored and transmitted to a vendor in most cases
- Currently user usually has control over whether feature is enabled (with some exceptions)
- Vendor largely controls how data is transmitted, stored and provided to other parties
Biometric Data Regulations in the US and Other Regions

Data Privacy in regards to Biometric Data is not highly or consistently legislated and regulated in the US
- No federal laws exist that require businesses to take specific actions in the collection and processing of Biometric data. A few laws exist that address specific instances such as the Family Educational Rights and Privacy Act which addresses collecting and releasing Biometric information of students
- Several states have laws governing or prohibiting the use of Biometric data in connection with drivers licenses
- Illinois and Texas have enacted laws regulating private entities use of Biometric information and several other states have introduced similar legislation
- The Illinois Biometric Information Privacy Act (BIPA) creates a right of private action against business that do not comply with the act. This type of legislation is likely to increase

Data Privacy in regards to Biometric Data is highly legislated and regulated in many regions outside of the US
- The EU GDPR (General Data Protection Regulation) will take effect in May 2018 and replace the EU Data Directive
- Article 9 requires individuals to give "explicit consent" for companies to use "special categories" of personal data including Biometric data
- Transfer of biometric data out of a jurisdiction is generally restricted
- The GDPR requires a "Privacy Impact Assessments (PIA)" for processing Biometric data
Question: Is Biometric data considered Personal Data, Public, Private, Restricted, Sensitive, Confidential?  **Answer: Yes?**

Examples of Biometric Data include:
- Fingerprints, Iris patterns, retina scans, facial recognition, DNA, voice, etc.
- Biometric data is generally considered personal data as it can be used to confirm the unique identity of a user and therefore the processing of this data is generally subject to data protection and privacy laws.

The fact that the data is considered personal does not by itself determine how an organization should protect the data.

A Privacy Impact Assessment (PIA), rather than a "label", is the key to understanding threats, risks and the associated controls that should be implemented.
Privacy Impact Assessment

- A privacy impact assessment can determine the confidentiality, integrity and availability requirements for each Biometric data element based on business, technical, legal and regulatory requirements

Examples (for demonstrative purposes only):
1) Facial Recognition Pattern used by mobile banking application
   Confidentiality Requirement – Medium (this data needs to be protected, but is generally publically available and can't be easily used for malicious purposes)
   Integrity Requirement – High (changing of this information could result in unauthorized access to financial data)
   Availability Requirement - Medium (secondary authentication methods are available)

2) Retina Scan used to access a secure data center
   Confidentiality Requirement – High (retina scans can be used to identify chronic health conditions and may be subject to HIPAA regulations)
   Integrity Requirement – High (changing of this data could allow unauthorized access to a secure facility)
   Availability Requirement – High (this is the only authentication method allowed and must always be available)
What are the implications of the disclosure of Biometric data to unauthorized individuals?

**Disclosure Example:**

Office of Personnel Management (OPM) 2015 Data Breach: 5.6 million fingerprints were stolen as part of the attack
- Unlike passwords or even social security numbers Biometric data can never be changed
- No uniform standards exist for securely storing Biometric data and the fingerprints that were disclosed were not encrypted in any way
- This seems really bad

But...

- What can someone do with this data?

Right now the potential for misuse of stolen fingerprints is limited as an attacker must be able to inject this data into the information flow of an authentication transaction

The potential for misuse will likely increase in the future as Biometric authentication becomes more common and the data is more widely used

*This leads to the next question which is:*

*If it is really hard to do anything malicious with this data does that mean we don't really have to worry about how well it is protected?*
Why do we need to protect Biometric data and do I really care if my fingerprint is "stolen"?

- The prior slide showed that the risks associated with the disclosure of Biometric data may not always be high (putting regulatory requirements aside) especially for data such as facial scans or even fingerprints that can be obtained relatively easily and don't divulge any sensitive details about an individual.

But.....

We also need to consider the integrity and availability of the data and what could happen if the integrity or availability is compromised?

- What if your fingerprint that was sent to the FBI for a criminal background check was accidentally added to the criminal database instead of the civilian database?
- What if a known terrorist or criminal fingerprint or other biometric data was destroyed or replaced with your data?
- What is the only way to access a secure facility is through Biometric authentication and the system is not available?
- These examples clearly illustrate that the confidentiality, integrity and availability of Biometric data all need to be equally considered.
Do you believe that you should control how your Biometric data is captured and used?

Most people believe:

- They should have to consent to have their biometric data collected, stored and distributed
- They should have the right to know exactly how their data is being used and that it is stored and transmitted securely

but this is a complicated issue and the fact that the privacy of Biometric data is not highly legislated and regulated in the US creates interesting questions that need to be considered such as:

- If you are hired by a financial institution and subject to a background check and fingerprinted do you know where that data goes and who has access to it?
- Do you need to give permission for a bank to take and store your picture when you are performing a transaction at an ATM?
- Do you know what the DMV is allowed to do with the facial recognition data that they store and which agencies they can share the information with?
- Can the FBI collect and store publically available pictures that are available on Facebook?
- If you have been to Disney World have you thought about what they do with your finger scan data? **

** Disney doesn't actually capture fingerprints. They take a biometric measurement based on your fingers size and proportion.
Social Implications of Broad Biometric Adoption

Hmmmmm this could be a problem....

Biometrics can be an enabling technology, especially for individuals with disabilities (i.e. someone that can't type a password), but only if it is used correctly.

Many social factors need to be considered for Biometrics to be successful on a global level or for a company to make Biometric authentication mandatory rather than an option.

Social Adoption Considerations:
- Long fingernails are highly valued in some cultures and communities which must be considered when using finger scanners
- An individual may not want to place their finger on a scanner for fear of catching a disease
- Some individuals simply don't like to have their picture taken
Social Adoption Considerations (continued):
- Individuals may be reluctant to use Biometrics if they don't trust the entity that will be collecting and storing the data
- Individuals may have doubts about the accuracy of Biometric data and concerns about how the data will be used now and in the future
- In emergency situations individuals may need a trusted individual (child/parent, etc.) to perform a transaction on their behalf. How many people have ever given their card and PIN to a spouse or child?
- People may have concerns that the Biometric data will be used for research or other purposes that they don't believe in
- Some Muslim cultures prohibit women from being seen without a veil
- Certain individuals may dress in a manner that makes it difficult see facial features clearly such as wearing head coverings or hats
Examples of Current Privacy Concerns

May 2016 - Facebook faces privacy lawsuit over photo tagging: Facebook is being sued in a case alleging that its photo-tagging feature that uses facial recognition technology invades users' privacy and violate the Illinois Biometric privacy laws. In May a federal judge rejected Facebook's request to have this lawsuit dismissed.

December 2015 - Bangladesh introduces mandatory Biometric registration for all SIM card owners: With this new system every mobile SIM will be associated with its users identity as it appears in the national identity card system. This will potentially give the government unprecedented oversight into the lives of Bangladeshi citizens. It is not clear which laws will govern the use of this data.

April 2016 – Oklahoma moves to enact law to accommodate religious objections to Biometric photo requirements on Drivers License: In April 2016 reinstated this lawsuit which alleged that requiring a Biometric photo as a condition for obtaining a drivers license violated Oklahoma's Religious Freedom Restoration Act.
Examples of Current Privacy Concerns: FBI Next Generation Identification (NGI)

- The Next Generation Identification (NGI), provides the criminal justice community with the world’s largest and most efficient electronic repository of biometric and criminal history information.
- National Palm Print System (NPPS). This system contains palm prints that are searchable to law enforcement nationwide. The NGI System also allows direct enrollment and deletion of palm prints and supplemental fingerprints similar to the existing direct fingerprint enrollment capability.
- Rap Back - The Rap Back service allows authorized agencies to receive notification of activity on individuals who hold positions of trust (e.g. school teachers, daycare workers) or who are under criminal justice supervision or investigation.
- Interstate Photo System (IPS) - The IPS, through facial recognition, now provides a way to search millions of criminals’ photos—data the FBI has collected for decades.
FBI Next Generation Identification (NGI) Privacy Concerns

- The 2015 omnibus budget, for example, includes $117 million for the purchase of rapid DNA testing machines for state and local law enforcement. The FBI runs the nation’s largest DNA database, CODIS. Therefore state and local police who obtain these machines will use them to send DNA samples to the FBI database for matching tests. Presumably, like with other biometrics, the FBI will keep those records, thereby exponentially expanding its DNA collection on people nationwide, many of whom will never be convicted of any crimes.

- The FBI recently issued a request for quotations (RFQ) to build out its mobile biometrics capabilities. Specifically, it’s looking for software that can be used on small Android-based mobile devices like Samsung Galaxy phones and tablets to collect fingerprints and face images from anyone officers stop on the street.

- The biggest concern with this new mobile program is that it appears it will allow (and in fact, encourage) agents to collect face recognition images out in the field and use these images to populate NGI—something the FBI stated in Congressional testimony it would not do.
FBI Next Generation Identification (NGI) Privacy Concerns

• New Report: FBI Can Access Hundreds of Millions of Face Recognition Photos
• Today the federal Government Accountability Office (GAO) finally published its exhaustive report on the FBI’s face recognition capabilities. The takeaway: FBI has access to hundreds of millions more photos than we ever thought. And the Bureau has been hiding this fact from the public—in flagrant violation of federal law and agency policy—for years.
• According to the GAO Report, FBI’s Facial Analysis, Comparison, and Evaluation (FACE) Services unit not only has access to FBI’s Next Generation Identification (NGI) face recognition database of nearly 30 million civil and criminal mug shot photos, it also has access to the State Department’s Visa and Passport databases, the Defense Department’s biometric database, and the drivers license databases of at least 16 states. Totaling 411.9 million images, this is an unprecedented number of photographs, most of which are of Americans and foreigners who have committed no crimes.
• The FBI has done little to make sure that its search results (which the Bureau calls “investigative leads”) do not include photos of innocent people, according to the report. The FBI has conducted only very limited testing to ensure the accuracy of NGI’s face recognition capabilities. And it has not taken any steps to determine whether the face recognition systems of its external partners—states and other federal agencies—are sufficiently accurate to prevent innocent people from being identified as criminal suspects. As we know from previous research, face recognition is notoriously inaccurate across the board and may also misidentify African Americans and ethnic minorities, young people, and women at higher rates than whites, older people, and men, respectively.
FBI Next Generation Identification (NGI) Privacy Concerns

- FBI Wants to Remove Privacy Protections from its Massive Biometrics Database
- Next Generation Identification (NGI) Database includes fingerprints, face recognition, iris scans and palm prints—collected not just during arrests, but also from millions of Americans for non-criminal reasons like immigration, background checks, and state licensing requirements. The FBI wants to exempt this vast collection of data from basic requirements guaranteed under the federal Privacy Act
- EFF, along with 44 other privacy, civil liberties, and immigrants’ rights organizations, sent a letter to the FBI demanding more time to respond.
Thank You