# Private Sector Uses of Biometrics: From High-Stakes Testing to Loyalty Cards

Prepared for the

National Defense Industrial Association
Biometrics Conference

January 21, 2010

Kathy Harman-Stokes, J.D., CIPP

U.S. & International
Data Protection & Privacy Law

+1.703.216.5643 direct
kathy@stokes-law.com

# Private Sector Use of Biometrics: From High-Stakes Testing to Loyalty Cards

- High-Stakes Testing: Preventing Fraud in the GMAT® Exam
- Advances in Employee Access Control, Time & Attendance Tracking
- Biometrics to Secure Data at Data Level: Protect Every Mouse Click
- Consumer Authentication/Identification
  - Biometrics in Banking
  - Biometrics at Retail Point of Sale
- Biometrics in the Hands of Consumers

# High-Stakes Testing: Preventing Fraud in the GMAT®

- Scores used by 1900+ schools in 70 countries
- Delivered in 110 countries to approximately 250,000 people annually
- 2003: 6 individuals impersonated 185 business school applicants
- Exam fraud = fraud on the schools using scores. Unethical applicant gets in, honest applicant left out
- 2006: Began biometric fingerprints
- Process:
  - First time test taker provides print at test center check-in.
  - Upon returning from break, new fingerprint compared to original, 1:1
  - If person re-tests, new print compared to original, 1:1
  - If no match, manual investigation.

# High-Stakes Testing: Preventing Fraud in the GMAT®

- Yet, technical challenge with fingerprint
- Legal challenge: Strong cultural sensitivity to fingerprints, based on Nazis, Stasi/secret police.
    - In Europe, right to privacy is “fundamental human right,” basis of civil society, democracy
    - Embedded in national constitutions, European and EU law
    - Data collection, use and transfer out of EU highly regulated
    - Overriding EU law, plus national laws, with independent data protection authorities (“DPAs”) with varying powers
    - DPAs provide check on private and public sectors
    - Fingerprints rejected by some European authorities
- 2009: Shift to Fujitsu palm vein biometric

# High-Stakes Testing: Preventing Fraud in the GMAT®

- Palm vein system designed to meet challenges:
  - 1:N matching on the horizon
  - "No trace": User leaves no trace on device and no surreptitious collection
  - No image stored for later use
  - Unique algorithm to prevent interoperability
- July 2009: France's authority, the "CNIL," approved GMAT's collection, 1:N matching, and transfer of data into central database in the US
- Most other EU countries expected to follow
- Palm vein implemented in over 100 countries

# Biometrics for Employee Access, Time, Attendance

- **Global Rainmakers**: Iris Recognition System
  - High throughput while person in motion (up to 50 people/minute)
  - Ex: Large US bank using for employee building/logon access
  - Quick efficient system for 1:N
  - Less public resistance than w/fingerprint

© Global Rainmakers, Inc.

*Ex: Employee access through turnstiles*

- **Aurora**: Face Recognition System
  - Solved lighting problem using infra-red
  - Almost 100 clients, 940 sites in UK and Middle East: e.g., construction industry, colleges, airport operators using for 1:1
  - Ex: Engineering company using for employee access, time/attendance, with data passed to timesheet and payroll systems
  - Ex: Colleges using to track students’ attendance

# Securing Data at the Data Level: bioLock

- bioLock: Only SAP certified biometric system
- Secures HR, financial, health, research and other data at the data level, mitigating fraud and ID theft
- Protect any mouse click
- Swipe fingerprint on keyboard or mouse for 1:N identification for:
  - Initial computer log on
  - To view or edit particular data, e.g., employee/customer health info, financial records
  - For standard workflow approvals, e.g., manager approval of budget
  - To authorize a transaction, e.g., authorize wire transfer

# Securing Data at the Data Level: bioLock

- Blocks access for those not authorized
- Logs every attempt, identifies anyone in the system
- Reduce or eliminate reliance on passwords, risks of phishing
- Strong solution for Sarbanes-Oxley financial controls and HIPAA compliance
- Current users of bioLock include:
  - Major EU bank, other banks
  - European and US energy companies
  - European hospitals
  - California state universities, city governments

# Biometrics for Customer Authentication/ID

- National Australia Bank: Voice Recognition
  - 35 million customers. Significant losses from fraud, e.g., phishing, trojans, “man in the middle” trojans, ID theft
  - 2009: launched voice recognition for phone banking
  - Starting w/customers who cannot remember PIN code:
    - Previously, manual, time-consuming process. Ask 5 pre-selected questions.
    - Answers to questions now available on Facebook (e.g., high school mascot). Expansion of social networking leading to expansion of fraud, ID theft
    - Now, 85-90% of these customers enroll in voice recognition for 1:1 authentication.
  - VR enrollment is manual process, repeating info for print creation

# Biometrics for Customer Authentication/ID

- National Australia Bank:
  - Post-enrollment, customer calls automated system: if no PIN, put into VR system
  - Customer says NAB known ID number and DOB
  - System matches what is said for accuracy: correct NAB ID and DOB?
  - And matches whether voice print matches that NAB ID and DOB
  - 50K enrolled customers; exploring offering to all customers
  - Better customer experience than 5 questions; saves staff time/costs
  - With other security improvements, substantial reduction in fraud losses
- Several Japanese Banks: Palm Vein on ATMs

# Biometrics for Customer Authentication/ID

- EasySecure, Netherlands: Fingerprints at Retail Point of Sale
    - Fingerprint system authenticates customers, allows access, charges to account or as loyalty card
    - Manual enrollment process, web-based application
    - Allows 1:1 or 1:N matching
    - Post-enrollment, customer scans fingerprint, system checks against central database to authenticate or identify, approves or denies
    - Ex: At fitness centers, swimming pools, fingerprint allows access according to subscription
    - Ex: Camping store sets up customer account tied to fingerprint; allows charges via fingerprint from family
    - Ex: As loyalty card, fingerprint tracks purchases or points
    - No image retained; image retention generally now allowed in NL or Belgium

# Biometrics in the Hands of Consumers: Face Recognition Applied to Photos

- Apple® iPhoto ® "Faces," Adobe ® PhotoShop ®, other photo-sharing web sites group photos by faces
- Consumer's photos added to photo site
- Site software applies FR biometric technology to all photos, grouping together photos of people with the same faces
- Consumer adds names to each group of faces
- Convenient tool for consumers – easy to create albums for friends, family
- Possibly millions of biometric FR templates stored on web-servers through sites

# Conclusion

- Biometric use spreading rapidly in private sector – employees, and also retail and consumer applications
- Increased convenience, more accurate information, reduces employer admin costs
- But, what recourse if biometric data/ID stolen? How is data being used, by whom?
- Privacy and legal questions: In the US, not aware of any specific oversight or laws that apply to biometrics (except Illinois)
- Europe and US legal regimes share several common goals: fully inform consumers, give them choices, abide by their choices
- Europe: Strong rules and limits around biometric data use
- US: Goals met sporadically, case by case. Some disclosure and choice, determined by company. Do consumers fully understand? Limits on biometric use?
- As growth continues, when a major problem arises, regulation likely

# Kathy Harman-Stokes, J.D., Certified Information Privacy Professional

Kathy is an attorney and consultant on US and international data privacy laws, advising a broad range of clients on privacy laws, focusing on biometric laws. She advises her clients on, among other things, legal issues arising from the use of biometrics in specific countries, how systems should be designed to comply with international laws and where and how biometric data may be transferred. For 6 years, she was the Associate General Counsel and a corporate officer at the company that owns the GMAT exam, a high stakes test used for graduate business school admission worldwide. Kathy oversaw legal compliance efforts for the GMAT's collection of fingerprints and palm vein biometric data in 110 countries, and held discussions with EU data protection authorities concerning biometrics and other sensitive data. Before her work with the GMAT, she was an attorney at Hogan & Hartson LLP in Washington DC and McLean Virginia, specializing in litigation, employment and intellectual property matters. She attended the University of Virginia School of Law, and is an IAPP Certified Information Privacy Professional*.

**Note:** *The Virginia State Bar has no procedure for approving certifying organizations.*

Apple® and iPhoto® are registered trademarks of Apple, Inc. Adobe® and Photoshop® are registered trademarks of Adobe Systems Incorporated. GMAT® and the Graduate Management Admission Council® are registered trademarks of the Graduate Management Admission Council®.