

# CTO Corner

September 2011

## Has the Time Come for Mainstream Adoption of Biometrics?

*Dan Schutzer, CTO, The Financial Services Roundtable*

Biometrics<sup>1</sup> is a technology that has been poised to join the mainstream for over two decades, but until now it has not seen large scale deployment in mainstream markets except for niche applications. Has its time finally come?

There is a confluence of events that may result in biometrics finally beginning to gain wider acceptance in the marketplace. These enablers are summarized below:

### Smartphones and tablets are becoming biometrics-ready.

With the advent of smartphones there is now a device capable of having built-in biometrics; they already contain the necessary hardware for facial and voice biometrics (e.g. cameras and microphones with high enough resolution and fidelity).

### Popular applications are beginning to offer biometrics.

Now popular applications are beginning to be written that employ biometrics using this hardware. For example, Facebook<sup>2</sup> and Google<sup>3</sup> are starting to offer mobile applications that make use of facial recognition. They are being designed to help people find friends and improve their ability to know who they are interacting with. Other biometrics hardware and application software (e.g. iris and fingerprints) are also likely to become available, further down the road.

Having built-in applications, available at little or low cost, should help make biometrics more familiar, better understood and more likely to be used by mainstream users. In order for these applications to gain acceptance they will have to address privacy concerns, and provide the user appropriate education and controls. As familiarity with biometrics increases, its performance continues to improve, and privacy concerns get addressed, available biometric apps will increase in popularity, value and use.

---

<sup>1</sup> **Biometrics** (or **biometric authentication**)[\[note 1\]](#) consists of methods for uniquely recognizing humans based upon one or more [intrinsic](#) physical or behavioral [traits](#). In [computer science](#), in particular, biometrics is used as a form of [identity access management](#) and [access control](#). It is also used to identify individuals in groups that are under [surveillance](#). <http://en.wikipedia.org/wiki/Biometrics>

<sup>2</sup> Facebook has recently embarked on a major photo tagging project and already has the largest collection of identified photographs in the world outside of a government. [http://www.pcworld.com/article/229870/facebook\\_photo\\_tagging\\_a\\_privacy\\_guide.html](http://www.pcworld.com/article/229870/facebook_photo_tagging_a_privacy_guide.html) or <http://tinyurl.com/3pbqmof>

<sup>3</sup> Google App Would ID Faces, Dish Out Personal Info, By [Matt Cantor](#), Newser, posted Apr 1, 2011 4:17 PM CDT, <http://www.newser.com/story/115420/google-facial-recognition-app-would-id-faces-give-personal-info-raising-online-privacy-concerns.html>

### Biometrics being deployed for ecommerce, fraud fighting and criminal apprehension.

Speaker recognition is already being offered in many call center applications. Many of these applications are now beginning to include speaker verification/identification. Other applications are being deployed involving the use of facial recognition<sup>4</sup>, fingerprints and iris<sup>5</sup> in criminal prosecution. Biometrics has also been introduced as part of new mobile payment schemes<sup>6</sup>. As their use grows, it will become more commonplace for people to expect and accept the use of biometrics in commerce and fraud prevention.

### The growing sophistication of fraud dictates the need for stronger authentication, additional layers.

An added impetus for financial institutions to employ biometrics as an additional component in their suite of layered fraud prevention and detection controls is the increasing success and sophistication of criminals and fraudsters. This does not mean we should drop passwords and IDs, or identity tokens, for biometrics, but rather biometrics could be welcomed as an added layer of security, especially if it is sufficiently unobtrusive and easy to apply. Note the latest FFIEC guidance<sup>7</sup> doesn't call for biometrics, but it does acknowledge the need for stronger controls and clearly outlines the need for a system of layered security. It repeats, as it should, the fact that virtually every authentication technique can be compromised. Biometrics, like every other security control, is not a silver bullet. It is not foolproof; it can make mistakes and be spoofed. But, if properly designed and integrated into a comprehensive system of security controls, biometrics should make significant contributions to fighting fraud and identity impersonation. As users and service providers gain a better understanding of biometrics' strengths and shortcomings, along with knowledge that it will not be relied upon exclusively but will be an added component to other security checks and balances, it should help address privacy concerns regarding its use and improve confidence in its performance.

### **What should an FI do?**

It seems inevitable that over the next few years biometrics applications should increase and grow in use. Initial applications will probably emphasize their value in helping users do things quicker, easier and better. Improving security will likely be a secondary goal. As biometrics begin to get more widely deployed, it is important that we remain alert to their potential and growing acceptance. We should track and monitor the user experience and acceptance of these applications, trying them out ourselves so we can gain first hand experience and knowledge with them. As biometrics move further into the mainstream and gain acceptance for social applications, we might consider piloting their use in more sensitive financial service applications. To be successful, the application of biometrics should not only be designed to improve security and strengthen authentication, but should result in an application that is easier and more convenient to use.

---

<sup>4</sup> Police to Use Modified iPhone for Facial Recognition, Tech Minute for Thursday, July 14, 2011, [http://www.myfoxboston.com/dpp/morning\\_news/my\\_tech\\_guy/110714-police-modified-iphone-facial-recognition](http://www.myfoxboston.com/dpp/morning_news/my_tech_guy/110714-police-modified-iphone-facial-recognition)

<sup>5</sup> [www.reutersreprints.com](http://www.reutersreprints.com), Police to begin iPhone iris scans amid privacy concerns

<sup>6</sup> More for the Mobile Money, Payment system FaceCash adds appeal for consumers and merchants, Apr 2011, By Michael Hartnett, <http://www.stores.org/STORES%20Magazine%20April%202011/more-mobile-money>

<sup>7</sup> [http://www.ffiec.gov/pdf/authentication\\_guidance.pdf](http://www.ffiec.gov/pdf/authentication_guidance.pdf), FFIEC Guidance, Authentication in an Internet Banking Environment