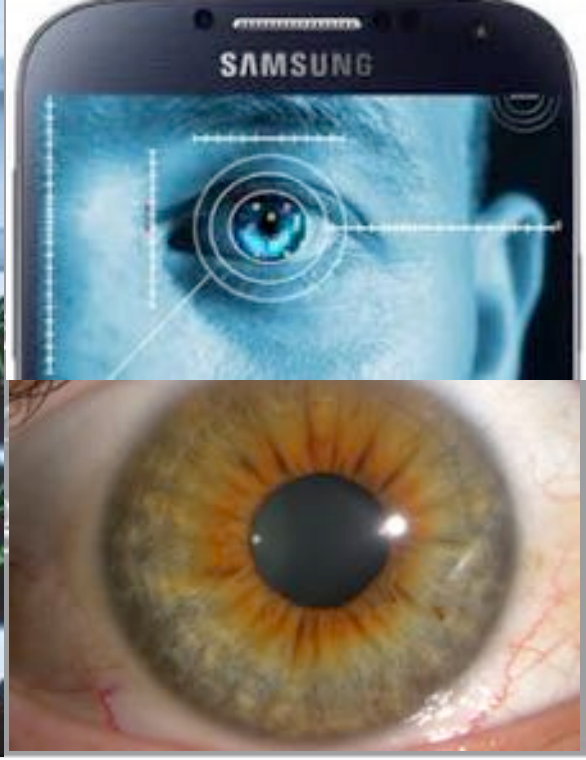


Biometric Technology & Smartphones

The Practicalities and Societal Impacts of a broad adoption of Biometrics – in our Smartphones!

Peter Corcoran | Nov 10, 20145

Overview – Main Topics

1. A Quick History + Introduction to Mainstream Biometrics
2. Practical Biometrics on Smartphones – Problems & Solutions
3. Identification Vs Authentication
4. Why Smartphones are the solution, not the problem!
5. The Risk of Identity Theft – is it real?
6. Biometrics and Privacy Concerns – who to trust?
7. Final Thoughts

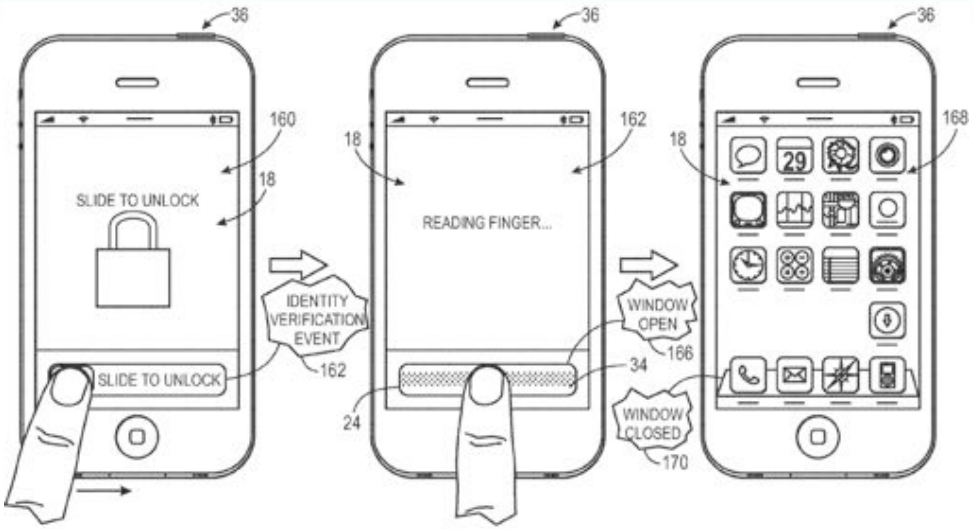
BIOMETRICS

A QUICK HISTORY + INTRODUCTION TO MAINSTREAM BIOMETRICS

There is Nothing New Here!

- Here is an iPaq from the early 2000's – one of the first functional devices with fingerprint ID.
- It was marketed to business users as a 'secure' device; but didn't last very long on the market!

So this should not surprise you!



- Re-purposing of the finger swipe operation that is used to unlock some devices.
- This Apple patent extends the concept to validate the user from their fingerprint and pre-dates Touch ID by several years.

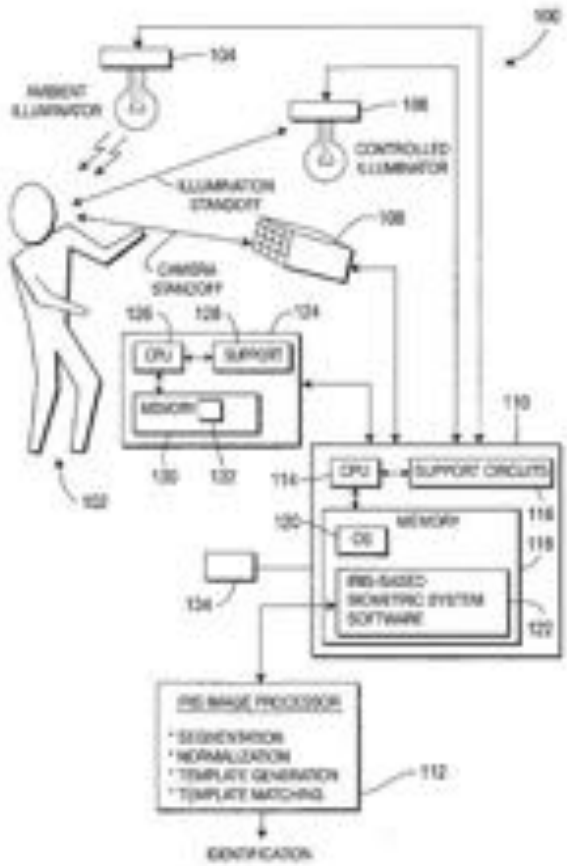
Main Biometrics – Jain et. al.

Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Palmprint	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Biometric Challenges

Can practical workflows & embodiments for biometrics be realized on today's handheld consumer devices?

- Well they already are on most of today devices!
- Apple uses **Fingerprint** to substitute for 5-digit PIN, but not sufficient for personal authentication;
- **Facial Recognition** has been tried but is unreliable & introduces privacy issues;
    - requires central database, or high levels of user trust
- **Iris** requires **InfraRed imaging** for reliable acquisition;
    - acquisition challenges, particularly with smartphone optics



PRACTICAL BIOMETRICS ON SMARTPHONES – PROBLEMS & SOLUTIONS

Iris Biometrics

Recent analysis, Proof of Concept and evaluation of the Visible/ NIR approach …

1. **Iris authentication in handheld devices-considerations for constraint-free acquisition.** Consumer Electronics, IEEE Transactions on, 61(2), 245-253. *Thavalengal, S., Bigioi, P., & Corcoran, P. (2015).*
2. **Proof-of-concept and evaluation of a dual function visible/NIR camera for iris authentication in smartphones.** Consumer Electronics, IEEE Transactions on, 61(2), 137-143.? *Thavalengal, S., Andorko, I., Drimbarean, A., Bigioi, P., & Corcoran, P. (2015).*
3. **Evaluation of Combined Visible/NIR Camera for Iris Authentication on Smartphones.** In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (pp. 42-49). *Thavalengal, S., Bigioi, P., & Corcoran, P. (2015).*

Our Conclusions on **Iris Biometrics**

- A challenging problem in terms of:
  - (i) Optical Design,
  - (ii) Sensor Resolution capabilities, and
  - (iii) User Workflow;
- Solvable but requires a lot of attention to detail;
- 'Industry' wants to see this Technology "in Play";
- Like it or not "iris authentication" is just around the corner!

Other Biometric Solutions

- **Fingerprint** – is considered less secure and requires more sophisticated hardware to achieve high levels of authentication;
- **Palmprint** – is practical with existing imaging technology, but not considered very secure; more prone to identity theft, etc.
- **Face Recognition** – is becoming practical with existing imaging technology but has similar issues with palmprint; our faces are already everywhere on the Web and can be easily captured while walking down the street!

It is likely we'll see mixed modes of biometrics …

IDENTIFICATION Vs AUTHENTICATION

Authentication is NOT Identification

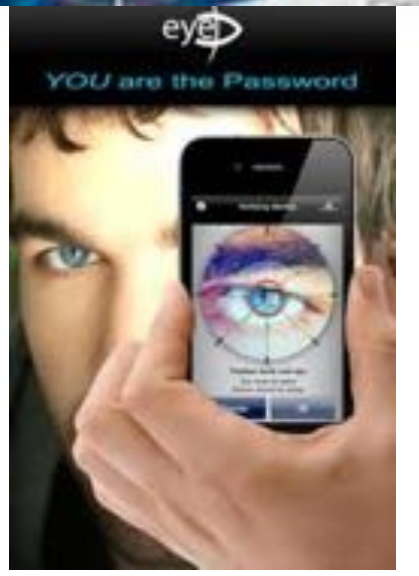
- We authentication ourselves regularly in our daily lives:
  - Sending e-mail to many people
  - Text messages from our phones and social media networks
  - Call people on the phone or over services like Skype
- Why do we trust E-Mail & Texts? How do we authenticate them?
  - You know the style of communication and writing (or TxTng)
  - The personal context of the message and communication
  - Most transactions have **no value** to parties outside the relationship

But Our Phones are becoming Targets!

- The Smartphone is key to your personal life:
  - Connects you to the 'Cloud'; your photos & movies;
  - Controls all your personal messaging;
  - Increasingly linked into your banking & financial life;
  - Very close to replacing credit cards for payments;

- For today it is enough to **trust your device** and assume it is still under your control – but for how long?



WHY SMARTPHONES ARE THE SOLUTION – NOT THE PROBLEM!

Biometrics & Smartphones

Smartphones can solve the problem of cancellable biometrics …

Soapbox Article – IEEE Consumer Electronics Magazine – April 2013

Biometrics and Consumer Electronics: A Brave New World or the Road to Dystopia?

By Peter M. Corcoran

Biometric systems confirm a person's identity by extracting and comparing patterns in their physical characteristics against computer records of those patterns. Examples include scans of the face, iris, or retina; measurements of hand geometry, palm or finger vein patterns; fingerprints, ear structure, voice patterns, or any other characteristic of the physical person that represents a unique attribute. The extracted patterns are matched against previously registered patterns, and, within certain tolerances, a confirmed match can be used to authenticate an individual's identity. In most practical systems, there is a need

processed to provide a unique identifying formula for each police offender.

First introduced into practical use in 1882, Bertillon's system was used in 1884 to confirm 241 repeat offenders in the Paris area. Its use was then widely adopted by the French police force. Although the system was later shown to be flawed because different police

People are generally suspicious of biometrics and, if biometrics are not introduced carefully into a

particular space and the placement of objects in it.

Fingerprinting is one of the earliest biometric techniques. In fact, fingerprints were used as signatures in ancient Babylon. However, the first scientific research began in the 17th and 18th centuries. Nehemiah Grew (1641–1712) published the first scientific paper to describe the ridge structure of the skin covering the fingers and palms [16]. A century later, in 1788, the German anatomist Johann Mayer (1747–1801) recognized that fingerprints are unique to each individual.

In modern times, fingerprints were first used as a form of legal authentica-

Smartphone Workflow #1

How the 'key' problems can be solved ...

- Biometric is acquired; may be intentional or background process
- Analysis and verification of the biometric – on the device;
- This process is partitioned from the main App Processor; it occurs in a secure computing environment where:
  - **Biometric** + private **device key** generate a public authentication key;
  - multiple device keys provide redundancy;

The only data that passes beyond the secure environment is the public authentication key;

Smartphone Workflow #2

Making the Biometric cancellable – without the complexity!

- The Biometric is never stored explicitly; the **match code** is stored in the secure environment;
- **Biometric** + **device key** are required to authenticate; even if you are victim of Biometric + device theft you can get a replacement device;
    - a cancellable Biometric without the complexity
- Still not convinced? Then use **Zero-Knowledge-Proof** techniques in combination!

Smartphone Workflow #3

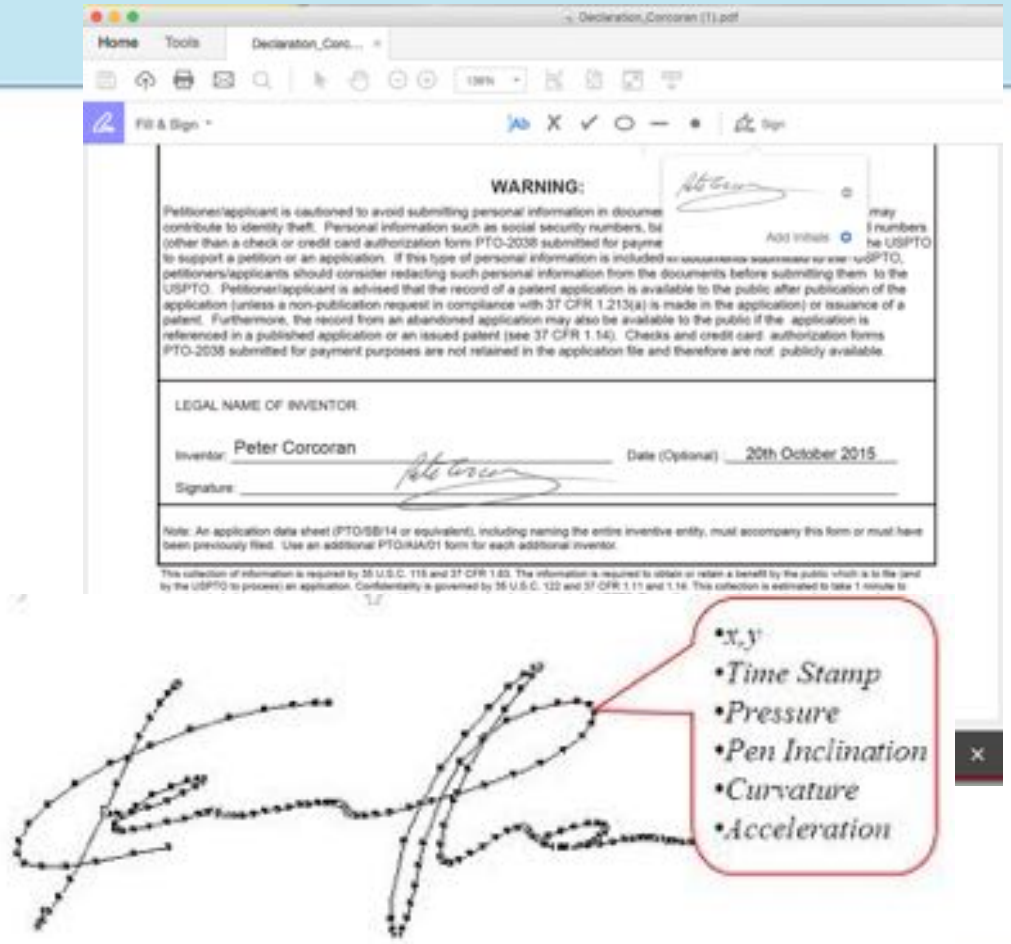
Continuous authentication – your device is constantly authenticating you!

- Our daily interactions with our devices provide multiple opportunities for authentication – faces, device handling, voice patterns, swipe and tap metrics, usage patterns for apps, etc …
- Explicit authentication is only required for transactions with a significant value – e.g. banking or online purchases;

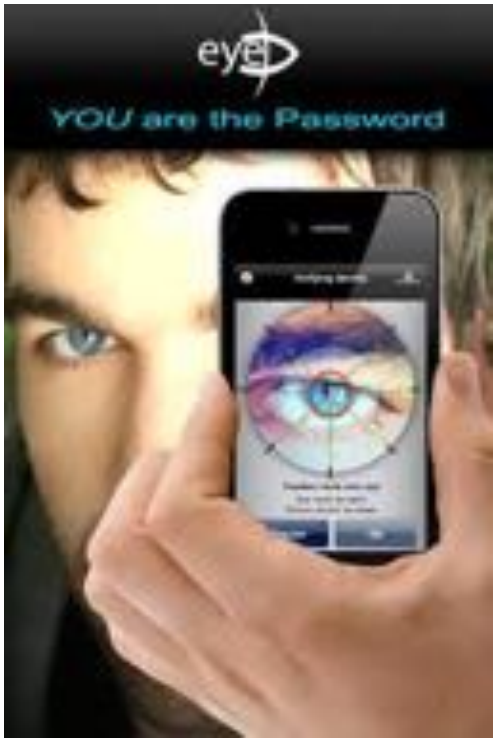
If you still think this isn't necessary then consider how easy it is to steal and re-use your handwritten signature!

Which is more secure?

Remember – your device can constantly authenticate you!



Vs



IDENTITY THEFT?

IS IDENTITY THEFT A REAL PROBLEM?

YOU NEED TO STEAL THE DEVICE AS WELL AS THE BIOMETRIC!

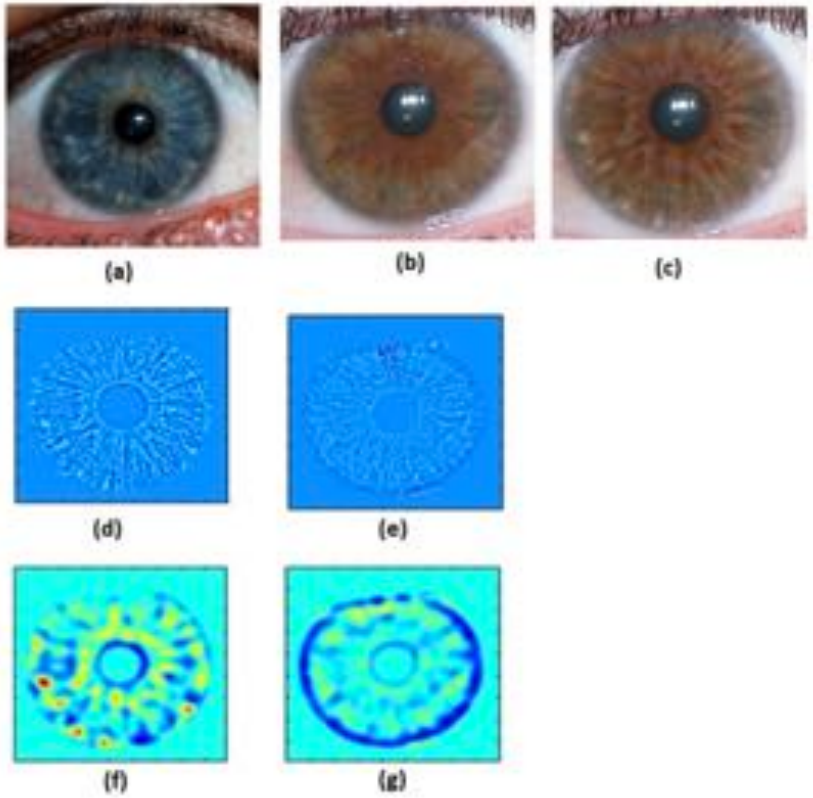
- **Liveness** testing is built into most Biometric acquisition techniques; remember that a smartphone is *acquiring images* before and after the main acquisition;
  - Faces must have depth;
  - Eyes need to blink;
  - Human skin can be tested for reflectance characteristics (with a flash);
- So **YOU** must be present;
- But in case you are not convinced there are other approaches:

Iris Obfuscation

Submitted to IJCB 2014 (*International Joint Conference on Biometrics*)

- Practical Approaches
  - Scramble Iris Pattern
    - But algorithms are too robust!
  - Blend another iris pattern into the eye (figure opposite)
    - Works well but privacy issues
  - Substitute randomly generated iris
    - Has to look realistic
  - Reverse engineer a pattern from the iris code
    - Quite challenging as code extraction is a 'lossy' process

Iris Replacement



PRIVACY ISSUES OF BIOMETRICS?

Governments & Corporations Love Biometrics …
… and lets be Honest – this is the real Concern!

Überveillance, the Web of Things, and People

What is the culmination of all this surveillance?

By M.G. Michael, Katina Michael, and Christine Perakslis

HISTORICALLY, TELECOMMUNICATIONS COMPANIES have measured voice and data traffic for reasons related to service dimensioning and engineering management. Today, personalized devices make it possible to understand not only the requirements for the capacity needed in a network but also household and individual usage patterns. This has changed the way that companies now market their products and services and sell directly to individuals. Beyond marketing is the intimate knowledge gathered of why people do things, inferred by pattern-of-life data and metadata. This is the precise knowledge of customer behaviors, traits, habits, and characteristics.

The Internet of Things (IoT) promises even greater connectedness as individual items begin to come alive on a global network, each with its respective IP address. Big data will soon be able to reveal patterns and trends that were previously incalculable. We will seek even greater levels of scrutiny in the not-too-distant future, heralding in an age of überveillance. We now know much more about consumers than traditional call holding times and the location of an individual user in a mobile network. Using evidence-based approaches, we can know what consumers are thinking, how they are feeling, and even what they will do next with a high degree of accuracy. Embedded surveillance devices will likely replace clunky mobile and wearable handsets and headsets, which will introduce an ability to transcend physical boundaries.

Digital Object Identifier 10.1109/MCE.2013.2306907
Date of publication: 9 April 2013

Psst...Your Location Is Showing!

Metadata in digital photos and posts could be revealing more than you realize.

By Katherine Albrecht and Liz McIntyre

A PICTURE MIGHT BE WORTH a thousand words, but someone can also pinpoint your X and Y coordinates on a map—even if you'd prefer otherwise. Just ask Internet security mogul John McAfee, creator of the famous McAfee Virus Scan software. His story illustrates how data embedded in digital photographs can lead to big trouble.

After making millions from the sale of his software company, the eccentric McAfee left the rat race and built a beachfront pleasure palace in Belize. There, the sexagenarian reportedly experimented with drugs, entertained young women, kept noisy dogs, and generally did his own thing.

He admitted his dogs annoyed the community, including his closest neighbor Gregory Faull, who often complained about the constant barking. When Faull was found murdered in 2012, the Belize authorities identified McAfee (whom they considered a gun-toting, drug-crazed madman) as a prime suspect.

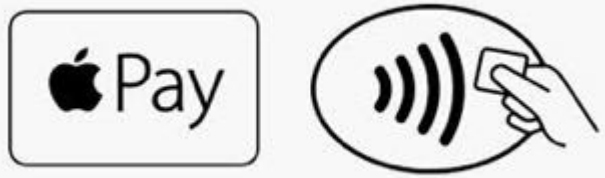
Digital Object Identifier 10.1109/MCE.2014.2306059
Date of publication: 17 December 2014

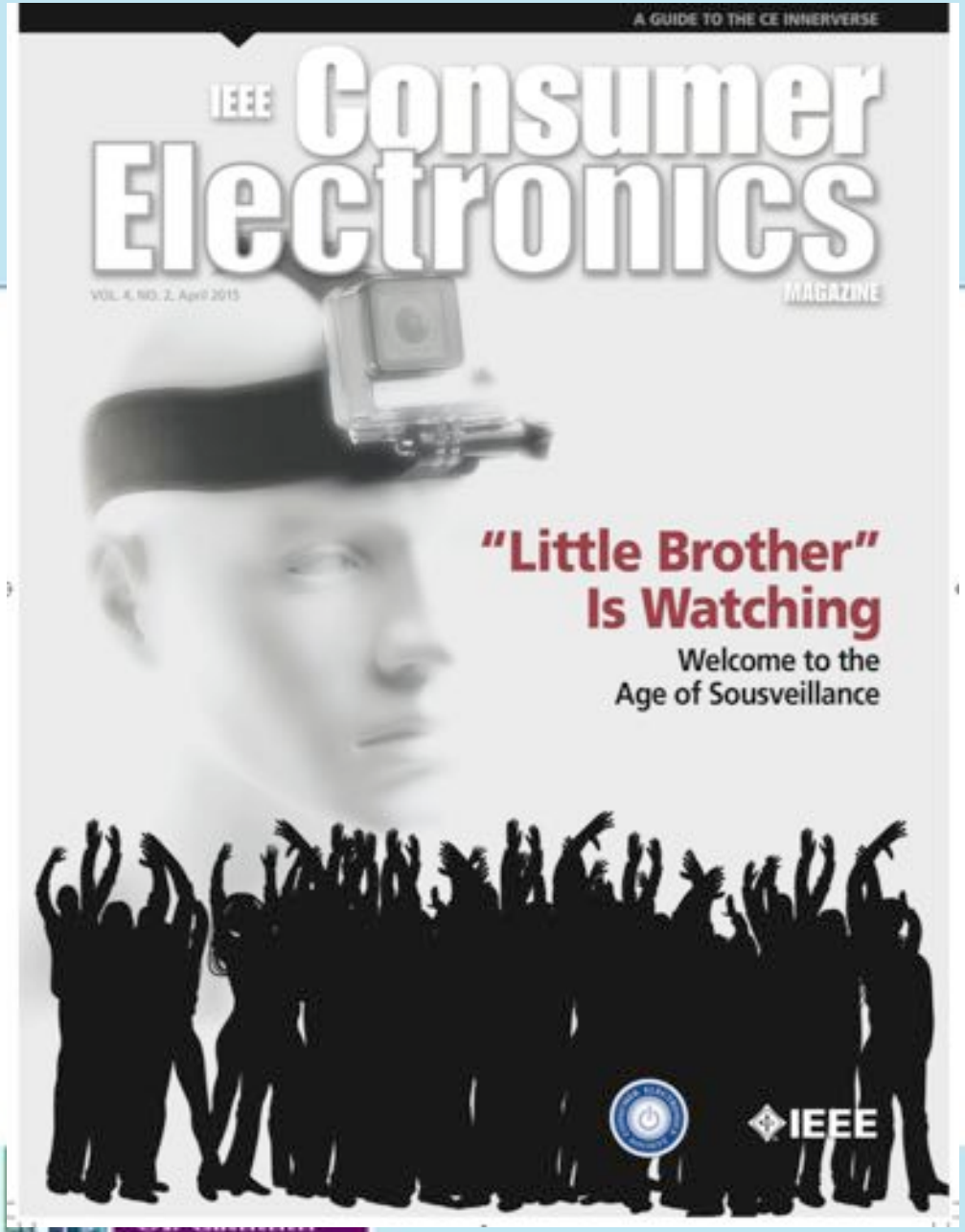
McAfee fled Belize to avoid arrest, using his fame and press connections to take highly publicized jabs at the police along the way. These taunts included an article in the online publication *Vice Magazine* titled, "We Are with John McAfee Right Now, Suckers" [3]. The story featured a picture of McAfee on the lam at an undisclosed jungle location.

When you are THE World's DATA HUB …

… You need the World's Biggest Data Center to store all that Cloud Data!

But Governments aren't the only ones who want you to trust them …

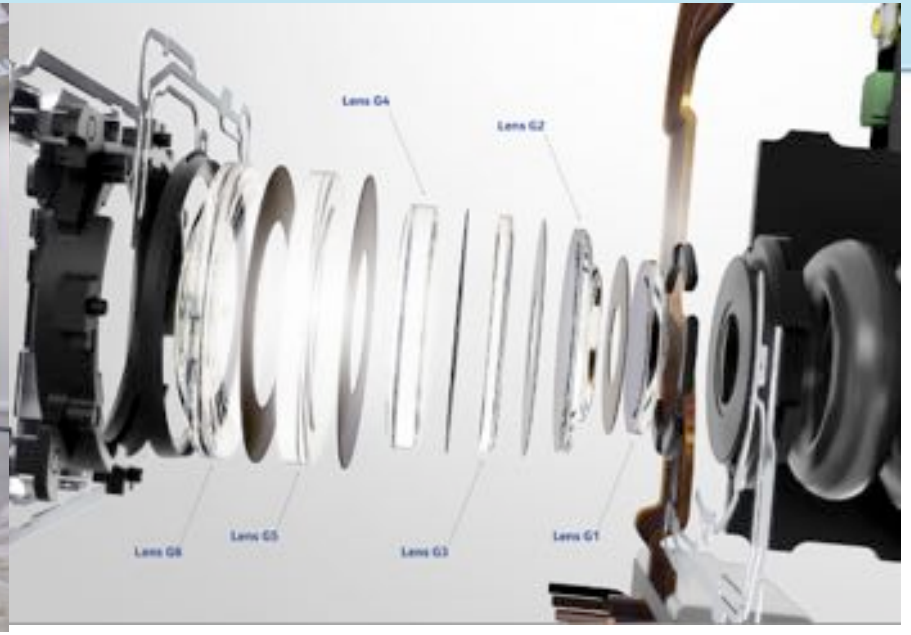




IEEE Consumer Electronics Magazine

April 2015 Issue –

Welcome to the Age of Sousveillance …



WRAP UP & QUESTIONS

Some Final Thoughts …

- We love our Smartphones and Biometrics will ADD very useful functionality …
- Industry does want to get the the use of Biometrics right so it will be adopted …
- ... And traditional means of authentication are fast becoming obsolete ...
- Authentication does not mean Identification …
- Do you prefer to trust Government or Google/Apple/ Microsoft?
- In-built Authentication can pave the way for other enhancement to Privacy and rights management …
- ... but is that a good thing?

???? QUESTIONS ????

BIBLIOGRAPHY

- Thavalengal, S., Bigioi, P., & Corcoran, P. (2015). **Evaluation of Combined Visible/NIR Camera for Iris Authentication on Smartphones**. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (pp. 42-49).
- Thavalengal, S., Andorko, I., Drimbarean, A., Bigioi, P., & Corcoran, P. (2015). **Proof-of-concept and evaluation of a dual function visible/NIR camera for iris authentication in smartphones.** Consumer Electronics, IEEE Transactions on, 61(2), 137-143.
- Thavalengal, S., Bigioi, P., & Corcoran, P. (2015)**. Iris authentication in handheld devices - considerations for constraint-free acquisition**. Consumer Electronics, IEEE Transactions on, 61(2), 245-253.
- Thavalengal, S., & Corcoran, P. (2015, January). **A practical challenge for iris authentication on handheld imaging devices**. In Consumer Electronics (ICCE), 2015 IEEE International Conference on (pp. 606-607). IEEE.
- Thavalengal, S., Vranceanu, R., Condorovici, R. G., & Corcoran, P. (2014, September). **Iris pattern obfuscation in digital images**. In Biometrics (IJCB), 2014 IEEE International Joint Conference on (pp. 1-8). IEEE.
- Corcoran, P. M. (2013). **Biometrics and Consumer Electronics: A Brave New World or the Road to Dystopia?[Soapbox].** Consumer Electronics Magazine, IEEE, 2(2), 22-33.