



## Smartphones, biometrics, and a brave new world

Title	Smartphones, biometrics, and a brave new world
Author(s)	Corcoran, Peter;Costache, Claudia
Publication Date	2016-09-09
Publisher	Institute of Electrical and Electronics Engineers (IEEE)
Repository DOI	<a href="https://doi.org/10.1109/MTS.2016.2593266">10.1109/MTS.2016.2593266</a>

# Smartphones, Biometrics and a Brave New World

---

P. Corcoran, C. Costache

<b>INTRODUCTION</b>	<b>1</b>
<b>THE AGE OF THE SMARTPHONE</b>	<b>2</b>
<b>BIOMETRICS – YESTERDAY AND TODAY</b>	<b>2</b>
<b>IDENTIFICATION VS AUTHENTICATION</b>	<b>3</b>
<b>ARE BIOMETRICS BAD?</b>	<b>3</b>
<b>BIOMETRICS AND BIG BROTHER</b>	<b>3</b>
<b>BIOMETRICS ON CONSUMER DEVICES</b>	<b>4</b>
<b>BIOMETRICS &amp; IDENTITY THEFT</b>	<b>4</b>
SPOOFING OF THE BIOMETRIC	5
SUPERVISED VS UNSUPERVISED AUTHENTICATION	5
<b>PRIVACY CONCERNS</b>	<b>6</b>
<b>AUTHENTICATING PEOPLE IN OUR DAILY LIVES</b>	<b>7</b>
<b>BIOMETRICS AND DAILY AUTHENTICATION?</b>	<b>7</b>
<b>AUTHENTICATION BY DEVICE</b>	<b>8</b>
<b>EN-PHONE ME BABY</b>	<b>8</b>
<b>THE ZEN OF ZERO-KNOWLEDGE-PROOF</b>	<b>8</b>
<b>MY PHONE, MY BIOMETRICS ... ALL MINE!</b>	<b>9</b>
<b>BIBLIOGRAPHY</b>	<b>10</b>
<b>LIST OF FIGURES</b>	<b>12</b>

## Introduction

The use of biometrics to identify people goes back more than 130 years ago to the work of an early pioneer from the French Police force - Alphonse Bertillon, who developed an anthropometric identification system for suspects in the 1880's. In popular fiction, Mark Twain wrote in "Life on the Mississippi", also in the 1880's, about how a murderer was identified by the use of fingerprint identification.

In more recent times biometric technology has become increasingly associated with Ubervveillance and tracking of the general populace. In particular science-fiction literature has tended to explore many fascinating dystopian futures and popular movies based on these tales have often been box-office successes and worked their way into the popular consciousness.

In this article we take a somewhat contrarian viewpoint – that biometrics may, in fact, offer solutions to many of the cyber-security problems that appear with increasing frequency in prime-time news. And this relies on the individual asserting ownership over his personal biometrics. A strange hypothesis, you might think – but let us start with the disruptive

technology that could enable this transition in how we view and use biometrics. Let start by considering that smartphone on your desk, or in your coat pocket.

## The Age of the Smartphone

In recent years the smartphone has experienced widespread global adoption across all demographics with the most rapid market growth in countries such as China and India. In parallel the technology has undergone rapid commoditization to the point where an entry-level, but fully functional device can be sold profitably for less than 100 USD opening new less developed markets in Africa and Asia. Ericsson's annual Mobility Report from Nov 2015 (<http://www.ericsson.com/res/docs/2015/mobility-report/ericsson-mobility-report-nov-2015.pdf>) reports that smartphones are expected to account for 6.4 billion mobile subscriptions in 2021, from the forecasted total of 9.1 billion mobile subscriptions. As a side note, the forecasted global population in 2021 is just under 7.8 billion. These trends suggest that society is moving rapidly to a point where practically everyone worldwide who lives in an urban environment will own a smartphone.

Or, perhaps more accurately, these devices will own us?

They are compelling devices that combine the capability to operate as a personal messaging hub, to provide mobile access to Web services, or sophisticated entertainment functions playing music and videos and most recently a personal broadcasting engine using new Web technologies [1], should you require such capabilities. And for many of us they have become the primary tool to record and document our personal lives in pictures and video.

According to a study made by O2 (UK mobile operator) in 2012, the smartphone has replaced a range of possessions: we use it now in place of alarm clock, camera, watch or desktop. In fact, according to the same study, making calls is only the 5th most used function of the smartphone with internet browsing topping the list. (<http://news.o2.co.uk/?press-release=making-calls-has-become-fifth-most-frequent-use-for-a-smartphone-for-newly-networked-generation-of-users>)

With the increasing capabilities of these devices, for many of us the smartphone has become the central focus of our lives.

The ability of a smartphone to augment our daily lives has already effected substantial changes in social behavior. For many years it was considered quite rude to leave your cell phone active in meetings; yet today it is quite acceptable to tap away at this gadget in your hand. Indeed it now seems to be considered impolite to interrupt someone while they are engaged in such (arguably) anti-social, tapping.

Like it or not we have entered the age of the smartphone.

## Biometrics – Yesterday and Today

Biometric systems are used to confirm or establish a person's identity by detecting, analyzing and then comparing patterns in physical characteristics against enrolled records of those patterns. Biometrics were initially introduced by French police officer Alphonse Bertillon, who developed an anthropometric identification system for suspects based on measurement of the characteristics of head and body and individual marks such as scars and tattoos (Figure 1). Examples of biometrics used nowadays include scans of the face, iris or retina, geometric measures of hand, vein patterns in the palm, patterns in the lines and ridges of the finger or palm, outer ear structure, audible voice patterns, or any characteristic of the physical person that can be quantified in a repeatable manner to provide a unique metric.

The extracted patterns are matched against previously registered patterns and, within certain tolerances, a confirmed match can be used to recognize an individual. In most practical systems there is a need for a large, centralized, data repository for storing the

registered patterns and substantial computing power is often required to process new patterns and compare these to the stored dataset.

## Identification Vs. Authentication

There are two main applications of any biometric recognition technology. When someone lays claim to be a specific person and a biometric is used to support this claim, this is verification or authentication of the individual. It is a “user-driven” technology in the sense that a person will normally volunteer their biometric in order to access a service or facility. The biometric is provided co-operatively and the process is open and in most current situations it is also supervised.

**Figure 1 - From Bertillon's Identification anthropométrique (1893), demonstrating the measurements needed for his anthropometric identification system (credit to Wikimedia Commons; image in public domain; [http://en.wikipedia.org/wiki/File:Bertillon\\_-\\_Signalement\\_Anthropometrique.png](http://en.wikipedia.org/wiki/File:Bertillon_-_Signalement_Anthropometrique.png)).**

As an example, consider when presenting a passport at border control - the agent compares your face to the picture in the document and manually verifies your biometric, in this case a picture of your face. This process is now replaced in some countries by passports with encoded biometric data and the manual verification is replaced with an electronic scan of the corresponding biometric – e.g. fingerprint, or iris codes. In others the biometrics are stored in a central database so the passport is, to some extent, moot as you are identified from your biometric – the passport isn't really necessary unless it is your first time to pass through border control.

Identification, on the other hand, is the task of determining an unknown person's identity. As an example, a police officer comparing a sketch of an assailant against a database of previously documented criminals to find the closest match(es) is an identification process. Identification systems are often implemented covertly without the user's knowledge. Practical examples in everyday use include scanning passengers at an airport terminal or train station, determining the players at a gaming table in a Casino, or cross-linking persons observed by street surveillance cameras with a police database.

## Are Biometrics Bad?

### Biometrics and Big Brother

Biometrics have a bad reputation, and it is easy to see why. They were developed to verify identity and the origins and almost exclusive use of biometrics until quite recently was in the field of forensic science. Biometrics were used to identify and verify that an individual had been present or associated with a crime scene. And subsequently they could be used to expose individuals who created false identities.

Biometrics of various forms featured frequently in science fiction literature and were explored by mainstream authors including George Orwell, Aldous Huxley, Philip K. Dick, Ray Bradbury and William Gibson. In most of these works biometrics were often viewed as serving to restrict and control the citizens and the portrayals of a society that employs biometrics are invariably quite negative.

These trends are continued in recent movies. In *Minority Report*, a movie adoption of a Philip K. Dick short story, the principle character is forced to have his eyes surgically replaced to prevent identification. In *Gattaca* a 1997 movie directed by Andrew Niccol, the principle character must carry samples of another person's genetic material with him on a daily basis to pass a range of authentication protocols. Rightly or wrongly literature and movies have most often portrayed biometrics as a key element in a dystopian society.

And the current reality continues this trend. The increasing use of public surveillance CCTV systems in airports, train stations and on the high street has introduced significant potential for covert observation and tracking of individuals without their consent. While there are arguably benefits to law enforcement and immigration officials, it is the covert and secretive manner in which such systems are operated that some members of the public find disturbing and that raise privacy concerns. Ironically many people provide open access to their location via their smartphones – arguably a far more pervasive invasion of privacy.

Interestingly it is a requirement of most such surveillance schemes that a centralized database of biometric characteristics is stored. This is a core weakness of these systems. Centralized data is easily targeted by cyber-criminals, a fact that becomes increasingly evident year-on-year. And the more valuable the data the more resources brought to bear in their efforts to steal that data. Big Brother might be watching you, but these days even Big Brother can have his pockets picked.

At this point it becomes important to distinguish between the willing use of biometrics by an individual to prove their identity (authentication) and the covert use of this technology without a user's knowledge or consent (identification). As readers of this publication will know the latter is often referred to as Ubertveillance. By making this distinction it becomes evident that most key privacy concerns are due to the role of biometrics in Ubertveillance. And most of us would agree that such usage is at best inappropriate and invasive. At worst it may be illegal and a violation of our fundamental rights.

Now having made this distinction a discussion can take place on the merits and benefits of the usage of biometrics for personal authentication rather than becoming unduly focused on the rights or wrongs of Ubertveillance. Biometrics, employed in the right context, can be both useful and solve a wide range of cyber-security issues for the individual and society. Yes, in the right context biometric technology could be good for you.

### **Biometrics on Consumer Devices**

It is only quite recently that the usage of biometrics was considered for applications beyond forensic, legal and specialized access control uses – more exactly, for authentication purposes on personal CE devices. Various systems to implement fingerprint biometrics have been available on handheld computers since the IPaq pocket-PC [1]–[3]. This featured a swipe fingerprint sensor and was available for several years in the early 2000's, but was eventually withdrawn from the market.

Fingerprint technology was featured on other consumer devices, including smartphones, but it was not until the introduction of Touch ID™ in 2013 that fingerprint recognition really came into mainstream consumer use. The Touch ID™ sensor uses capacitive touch to detect the user's fingerprint and has 500 pixels per inch resolution. The fingerprint can be read in any orientation – an important feature for consumer applications. It is closely integrated into the iOS operating system and the user's fingerprint can unlock the device and in addition authenticate purchases of digital media. The fingerprint data is stored locally rather than in a central database – an important point that will be discussed later.

**Figure 2. A close-up of the swipe fingerprint sensor (below the main central button) on an older IPaq handheld computer.**

### **Biometrics & Identity Theft**

Naturally the next concern stems from this use – if my biometrics can be used to prove who I am, then someone who can duplicate or steal them can easily become “me”. Fortunately this is a problem that has existed for some time and a significant amount of work has gone into consideration of the problem and almost as many proposals to solve it. Lets take a look at a sample of the most common approaches.

### Spoofing of the Biometric

It is almost impossible to have a conversation about biometrics without the mention of the potential to ‘spooft’ a person’s biometric.

There are measures that can be put in place to reduce the risk of direct theft of the biometric data. In the case of iris it has been proposed to implement an *obfuscation process* in imaging devices [4] to modify the iris patterns in any faces detected by an imaging device. This is not as farfetched as it might seem - many modern imaging devices incorporate real-time face tracking technology that enables to follow faces and features such as the eyes throughout an imaged scene.

**Figure 3. Example of iris obfuscation by iris pattern replacement. a) standard gallery iris (artificial), b) original image, c) output image of iris replacing technique**

Another defensive measure is the use of *liveness detection* methods. The smartphone is rich source of these as it is constantly interacting with the user and there are as many ways to verify a biometric as there are to spoof. Video sequences, for example, can be used to fake a user and can appear extremely realistic, but simply activating a LED or similar point source of light will provide an indication as an active glint in the pupil of the eye to show it if is a live eye, or a false video eye.

Secondary biometrics can further improve the robustness of biometric systems to potential spoofing attacks. Daugman has published results of studies involving the order of hundreds of billions of cross-comparisons of iris codes [5] showing that while one iris code might be duplicated across a large segment of the population, there is almost no statistical likelihood for a pair of people to have both iris patterns duplicated. This does not occur even in the case of identical twins. A similar logic follows if we use two different biometrics e.g. iris and palmprint, or iris and fingerprint. And using two complimentary methods of liveness detection can also reduce the scope for spoofing. Thus an analysis of the lips region of the face and a comparison with extracted word structures from an audio recording could be used as a *liveness* measure for speech detection. The speech itself and the voice characteristics could be used as a biometric.

And so while identity theft via stolen biometrics is feasible, it is far from trivial. And the challenges posed are only likely to grow more sophisticated in the future.

### Supervised Vs. Unsupervised Authentication

This is perhaps the biggest leap with smartphone biometrics – almost all other existing biometric systems employ a supervised authentication process. There is always a human overseer who can step in where the process fails. This is a luxury that is not available to the purveyors of consumer products and if the device does not perform as expected without the need for user supervision, it invariably ends back with the manufacturer.

A continual challenge with consumer systems is that everything is expected to work and to work consistently, even in difficult non-standard conditions. Looking back historically to the mid-2000’s when the first pocket-PC devices appeared with a sweep fingerprint scanner we can hypothesize that their short timeframe in the market was due to poor reliability of the fingerprint authentication system. While this was never admitted publicly it makes sense and the achievement of Touch ID™ in succeeding where others failed must be acknowledged [6].

The other challenge of unsupervised authentication is, naturally, that you are not around to detect when the ‘bad guys’ try to crack your authentication system. This challenge is less tested and there will definitely be a great deal of discussion and publicity directed here as biometrics becomes further embedded into mainstream devices.

But the use of biometrics is not less secure than many of the ‘manual’ systems used today to secure our credit cards and bank accounts. When a customer is requested to verify themselves on the telephone they are invariably asked a sequence of questions about their past

life – where they lived, their first car, their first pet, their best friend at school, mother’s maiden name and of course, their date of birth; this exact same information has been provided to tens, even hundreds of other companies, services and websites. Just one of these entities could have a dishonest employee willing to steal and sell on such data – how is this less a risk than committing one’s biometric data to a modern electronic device that sits in a jacket pocket most of the day? At least the user knows the device’s location 24/7 until they manage to lose it and even then they can get to a network and hit the kill switch.

And what if we return to the use of a personal signature as the legally binding baseline of authentication? Well how difficult is it to perform a high-resolution scan of your signature from a page and extract the corresponding bitmap image? And the latest version of Adobe PDF viewer allows you to import just such a bitmap to facilitate electronic signing of PDF documents! So which is more secure – an advanced biometric obtained using liveness detection to ensure that you were actually holding and operating the device, or your handwritten signature? I know where I’d prefer to put my money, literally as well as figuratively.

#### **Figure 4 Personal signature scanned in pdf Vs. Iris based authentication in smartphone**

### **Privacy Concerns**

This brings us to the topic of biometrics and privacy. If personal biometrics are to be used as a means of authentication it becomes critical to consider the use cases employed. Legacy biometric techniques gather data in centralized databases, and these ‘enrolled biometrics’ become a permanent record of your identity. Thus the owner of the data becomes the effective arbiter of your identity.

Clarke [7] has written in detail on this topic. He separates privacy into a number of sub-categories and emphasizes the need for safeguards depending on the particular use of biometric data. These safeguards are essential if biometric technology is not to fall into ill-repute even in relatively free societies. In more authoritarian societies he considers that the worst fears expressed in popular culture may well become reality.

Jain and Nandakumar [8] focus more on the maturity of biometric technology but recognize the importance of considering privacy in any particular application of biometrics. More specifically they raise several key concerns:

- “Who owns the biometric data, the individual or the service providers?”
- “Will the use of biometrics be proportional to the need for security in a given application? Should a user be required to provide a fingerprint in order to purchase a hamburger or access a commercial website?”
- “What are the tradeoffs between application security and user privacy? Should governments and businesses be allowed to use video surveillance in public spaces to covertly track the activities of users?”

There are many additional articles in the legal and philosophical literature that discuss various moral and ethical aspects of biometrics. But while biometrics are part of the discussion, it is increasingly clear that they are only one, relatively small facet of the broader discussion surrounding personal privacy. The broad adopting of Web and social media technologies combined with mobile Internet technologies are the central culprits here. They have spawned broad inter-generational shifts in our perceptions of and expectations with regard to personal privacy.

From the perspective of this discussion we consider the smartphone as the means to acquire and verify the biometric. There should be no need for the biometric to transfer beyond the device. In fact as we will see shortly, your smartphone provides an argument why your

biometrics do not need to be collected centrally. It removes the rationale for maintaining centralized databases, a key tenet of Ubervelance.

## Authenticating People in our Daily Lives

Most of us communicate on a daily basis using e-mail. Ironically e-mail represents an unsecured mode of communications that can be easily intercepted and/or spoofed but very few of us worry about this. And it does not happen very often. Did you ever wonder why not?

Well the economic value of the vast majority of e-mails to a 3rd party is negligible. More importantly the nature of the social and business activities that are mainly conducted over e-mail do not make it worthwhile to try and eavesdrop and analyze the vast volumes of 'noise' that we send to each other<sup>1</sup>. And the complexity of such interaction make it resource intensive to build convincing models that would enable 'fake messages' of economic value to be generated.

As a practical example, most of us receive regular phishing messages asking us to log into our bank or social network accounts. But only a small proportion of 'new' Internet users are fooled by such messages. And so we do not require additional authentication for most of our e-mail correspondence or phone communications because we *know the people* we deal with and they are identified by their e-mail address or phone number. In effect we accept an unsecured "machine identifier" to identify the person at the end of the communications link.

It is true that additional cues such as voice or message writing style are unconsciously anticipated and that aberrations or absence of the expected cues would immediately create suspicion; but the key point here is that the initial authentication is based on an unsecured machine identifier.

But we have to ask the question how much longer this will continue? Phishing attacks are getting smarter and more sophisticated; more and more people continue to join the global Internet community and there is an ever growing array of network based services that become increasingly integrated into our daily lives. How long is it before the economic value of your online presence grows to the point where it becomes a target for the growing army of cybercriminals? And in this nearer-than-you-think future you may no longer be able to trust simple "machine identifiers" as you do today.

## Biometrics and Daily Authentication?

If biometrics become commoditized in the near future, and this is a key hypothesis of this article, then you'd expect that incorporating your fingerprint or iris code into an e-mail would offer an elegant solution? Your laptop certainly has time to observe and scan your eye while you are composing that e-mail [9].

But a key problem with biometrics is that they cannot be revoked. The Electronic Freedom Foundation explains this very nicely (<https://www.eff.org/issues/biometrics>):

*"In the near future, biometrics could stand in for your driver license or social security number, and you could be asked for a thumbprint or an iris scan just to rent an apartment or see a doctor. This could lead to many vulnerable copies of that linked data that could wind up in the hands of identity thieves. And any data compromises would be catastrophic; unlike a credit card or even a social security number, your biometric data can't be revoked or re-issued."*

Thus if every e-mail you send has your biometric encoded into the mail signature it won't take too much effort for a cybercriminal to access your biometric codes. And at that point you are exposed to a risk of permanent identity theft. If you don't believe this, then you should

---

<sup>1</sup> There are significant exceptions, but we are mainly interested in consumer requirements, rather than those of business, enterprise or even national security.

know that the iris pattern can be reverse engineered from a simple binary iris code [10]. You can't change your biometric so the thief has got a permanent long-term access to your identity.

Once you understand this key point you'll realize why the widespread use of biometric data starts to raise so many concerns. There is a big Pandora's box here – biometrics are fixed permanent features and they can be copied and duplicated although it is not trivial to do so. So there is a big challenge here - if we get things right then biometrics could address a wide range of new and emerging problems. But the penalties for getting it wrong are huge and could precipitate a major societal catastrophe.

## Authentication by Device

So our initial considerations suggest that biometrics is not a practical solution that can solve tomorrow's authentication problems in a sustainable way. But could biometrics provide part of the solution? Is there a way to utilize and apply biometric technology that won't risk kickstarting a huge new segment of the cybercrime industry?

Well, consider that our smartphones are always with us, and they become increasingly integrated with our environment. Recently I noticed that my laptop is responding to phone calls before my phone (they are paired) so I found myself taking calls on my laptop as it was easier and faster than pulling the phone out of my pocket! The same linking occurs in my car and soon throughout my home. So could we take advantage of this to use our smartphones as engines to support personal Authentication?

### En-Phone me Baby

The problem of biometric theft becomes significant when you store a biometric pattern in a central repository or database, or if you encode it in a repeated e-mail signature or any regular data store. The sheer number of biometric signatures that can be obtained make these very attractive targets for cyber criminals. And if the rewards are large enough then they can find the seed financing and resources needed.

However, what if the biometric is used to generate an *enrollment key* and that is what is stored, rather than the biometric itself? Then this drawback is eliminated and if the key is stolen it is a straightforward process to generate and register a substitute *enrollment key*. But you need "something" to generate this key and this "something" must also be available later to decode the key and close the authentication loop. And that "something" has to be quite generic and widely available.

Is there some 'device' that practically every adult carries around with them every day that could perform that function?

Well it doesn't take a rocket scientist to realize that your smartphone can help here. They are always with us. And they are looking at us and listening to us on a daily basis. So capturing our physical characteristics is straightforward enough via our daily use of these devices. They can be repurposed to acquire a range of our biometrics through our daily use patterns and thus build a profile of the device user that can be used to continuously authenticate and where needed, authorize access to services and confirm transactions.

Brave new world here we come ...

### The Zen of Zero-Knowledge-Proof

You may still be uncomfortable that someone can break into your device and access your biometric data. In fact this concern is moot, because your device will never store your biometric data directly. Instead it will store a code derived from your data and the way it derives that code can, if necessary, be changed.

So all that your device really does is to verify that it has scanned your data recently and was able to generate the same authentication code(s). But there can be an additional layer of security here, because your device could store your authentication code in a secure memory and never export it. Instead it can use a well-known cryptographic technique - *zero-knowledge-proof* (ZKP) - to authenticate you to a network based service where you are enrolled [11]–[13]. This serves two purposes – the private key generated by your device, from your biometric, never leaves your device. In fact it will be secured in a special area of memory that cannot be accessed by the main device CPU.

The second reason to use ZKP is that the bulk of the cryptographic processing does not occur at the server – in fact the device has to do all the heavy computational work. The server creates challenges that only the associated client can solve using a private key generated from the user biometric. To increase the security level the server simply generates more sophisticated challenges for the client.

Although initially counter-intuitive it quickly becomes clear that there are some key advantages to this approach. Among these, the main cryptographic processes are not implemented on the network server and thus the attraction of obtaining millions of compromised access codes by breaking a single server-centric cryptography process is removed. Instead it becomes necessary to break a unique process for each device with the reward of a single access code. This does not justify the required scale & cost of resources.

A second benefit is in terms of scalability. As the main computational load is distributed across many individual devices the service can scale to many users without a need to add large amounts of computing power. And individual smartphones are now more than powerful enough to run the cryptographic solver algorithms in reasonable timeframes of several seconds or less. ZKP is an ideal match here as it keeps the most important functional elements of the cryptography distributed across millions of devices. And the reward for breaking the code on a particular device is limited to that single device. This acts as a strong disincentive for cybercriminals who can find easier pickings elsewhere.

## **My Phone, My Biometrics ... All Mine!**

And so we close the circle.

It is pretty difficult to lose your phone, but if you do it has become pretty straightforward to wipe it. Phone manufacturers understand how important our phones are to us and how much of our lives are entangled with these devices. And yes, they love this because it makes you a loyal customer – as long as they treat you with respect.

Enter biometrics. Easier to use than a PIN number and more reliable to authenticate the end user – their customer. After all, someone else can learn your PIN and use it to access your device; with a biometric is it not quite as straightforward, especially if the acquisition and analysis of the biometric happens on the phone itself.

But the really important part is that the biometrics used to authenticate you never have to leave your device. That eliminates the central database that can be targeted by cyber-criminals.

If we extrapolate a few years into the future, nobody needs a credit card – you can use a biometric-based access code paired with your credit account. That means no databases of customer credentials that can be stolen. Yes there is a database of ZKP enrollment keys identifying customers, but if you transmit those keys from a different phone, or with a different biometric then you won't be able to answer the ZKP challenges from the transaction server. The value of such a database is close to zero because of the level of effort required to exploit even a single enrollment key.

The end of online credit-card fraud as we know it?

And if your smartphone + your biometric become accepted to verify your identity for financial transactions, why not build on that to make it a legal instrument as well? Electronic documents could be signed with your enrollment key which would require your phone + biometric in combination to verify.

Of course there is always a flip-side to every story. This does require that we trust the phone manufacturers to keep our biometric data secure inside the device. We must trust in their algorithms and in the security of the transaction infrastructure implemented on their servers. And that they will provide robust mechanisms to back-up, secure and transition the enrollment keys generated on one device to a new replacement.

Yes, you can take back ownership of your biometrics and how they are used, but the trade-off is that you must trust the device manufacturer and their ecosystem.

But eventually you will have to trust someone. And as I write this, who is taking on the US Government in public court to fight for the right to a secure device? That is something that would not have happened even 10 years ago – but then again the modern smartphone isn't even 10 years old!

To conclude, let us consider the growing societal challenges posed to personal security and privacy through our networked techno-culture. This has shifted many of the ethical and culture norms that we have grown familiar with as a society, and in a relatively short time-span.

Ironically it is the most disruptive component of this new knowledge society, the smartphone that lies at the nexus of our techno-cultural evolution – while it has gathered many elements of our personal lives and laid these open for sharing and dissemination it has also brought the focus back onto the individual. And ultimately, these devices may return control to the individual citizen, offering appropriate solutions to manage and safeguard our personal security and privacy.

## Bibliography

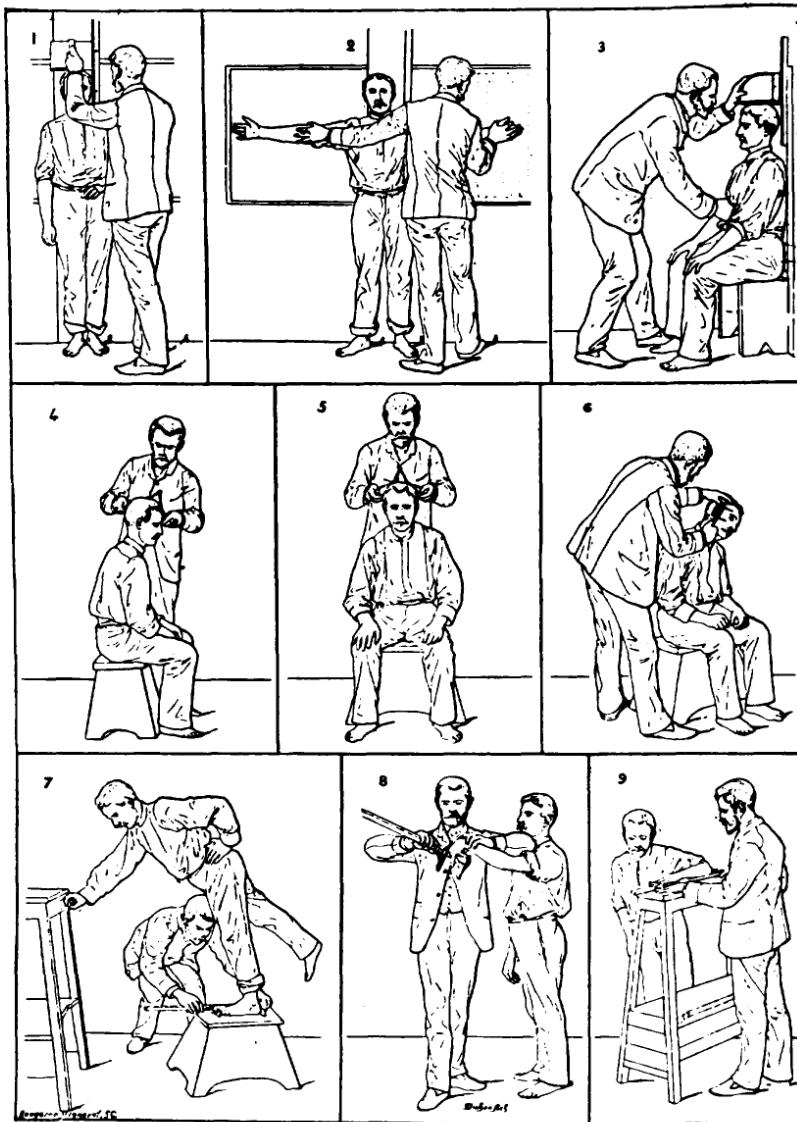
- [1] W. Jansen, “Authenticating users on handheld devices,” in *Proceedings of the Canadian Information Technology Security Symposium*, May 2003.
- [2] F. Callaly, C. Cucu, A. Cucos, M. Leyden, and P. Corcoran, “Real-time fingerprint analysis & authentication for embedded appliances,” in *Consumer Electronics, 2007 IEEE International Conference on*, 2007, pp. 1–2
- [3] C. Cucu, A. Cucos, and P. Corcoran, “Determining Unique Fingerprint Features for Biometric Encoding of Data,” in *Consumer Electronics, 2008. ICCE 2008. Digest of Technical Papers. International Conference on*, 2008, pp. 1–2
- [4] S. Thavalengal, R. Vranceanu, R. G. Condorovici, and P. Corcoran, “Iris Pattern Obfuscation in Digital Images,” in *International Joint Conference on Biometrics*, 2014, pp. 1–8.
- [5] J. Daugman, “Probing the Uniqueness and Randomness of IrisCodes: Results From 200 Billion Iris Pair Comparisons,” *Proc. IEEE*, vol. 94, 2006.
- [6] A. Goode, “Bring your own finger – how mobile is bringing biometrics to consumers,” *Biometric Technol. Today*, vol. 2014, no. 5, pp. 5–9, May 2014
- [7] R. Clarke, “Biometrics and privacy,” *Retrieved Novemb.*, 2001 <http://www.rogerclarke.com/DV/Biometrics.html>.
- [8] A. K. Jain and K. Nandakumar, “Biometric Authentication: System Security and User Privacy,” *Computer (Long. Beach. Calif.)*, vol. 45, no. 11, pp. 87–92, Nov. 2012
- [9] P. M. Corcoran, F. Nanu, S. Petrescu, and P. Bigioi, “Real-time eye gaze tracking for

- gaming design and consumer electronics systems,” *Consum. Electron. IEEE Trans.*, vol. 58, no. 2, pp. 347–355, 2012
- [10] S. Venugopalan and M. Savvides, “How to Generate Spoofed Irises From an Iris Code Template,” *IEEE Trans. Inf. Forensics Secur.*, vol. 6, pp. 385–395, 2011.
- [11] S. Grzonkowski and P. M. Corcoran, “A secure and efficient micropayment solution for online gaming,” in *Games Innovations Conference, 2009. ICE-GIC 2009. International IEEE Consumer Electronics Society’s*, 2009, pp. 118–125.
- [12] S. Grzonkowski, P. M. Corcoran, and T. Coughlin, “Security analysis of authentication protocols for next-generation mobile and CE cloud services,” in *2011 IEEE International Conference on Consumer Electronics -Berlin (ICCE-Berlin)*, 2011, pp. 83–87
- [13] S. Grzonkowski and P. Corcoran, “Sharing cloud services: user authentication for social enhancement of home networking,” *IEEE Trans. Consum. Electron.*, vol. 57, no. 3, pp. 1424–1432, Aug. 2011.

## List of figures

Figure 1

**RELEVÉ**  
DU  
**SIGNALEMENT ANTHROPOMÉTRIQUE**



1. Taille. — 2. Envergure. — 3. Buste. --  
4. Longueur de la tête. — 5. Largeur de la tête. — 6. Oreille droite. —  
7. Pied gauche. — 8. Médius gauche. — 9. Coudée gauche.

Figure 2



Figure 3

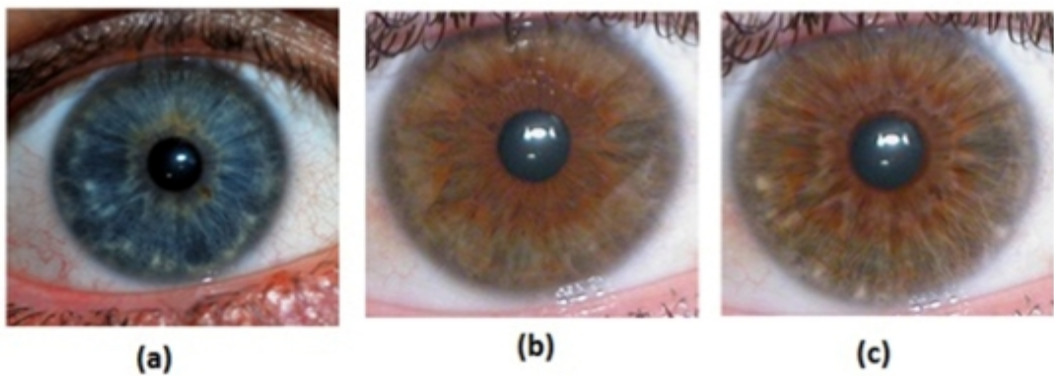


Figure 4

Declaration\_Corcoran (1).pdf

Home Tools Declaration\_Corcoran... x

138%

Fill & Sign

**WARNING:**

Petitioner/applicant is cautioned to avoid submitting personal information in documents contribute to identity theft. Personal information such as social security numbers, be (other than a check or credit card authorization form PTO-2038 submitted for payment to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Peter Corcoran Date (Optional): 20th October 2015

Signature: *Peter Corcoran*

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.111 and 1.14. This collection is estimated to take 1 minute to



Vs.

