Biometric Technology and Smartphones

A consideration of the practicalities of a broad adoption of biometrics and the likely impacts.

Peter Corcoran, Claudia Costache
Center for Cognitive, Connected & Computational Imaging,
National University of Ireland Galway,
Galway, Ireland
peter.corcoran@nuigalway.ie, claudia.iancucostach@nuigalway.ie

***Abstract*—The potential synergies between consumer handheld devices, particularly smartphones and biometric technologies is outlines. The practicalities and challenges for three such technologies – fingerprint, iris and palmprint – are presented. The use of biometrics for personal authentication is discussed, including the use of zero knowledge proof techniques to ensure that the biometric data does not leave the phone. The scope for data theft and breach through spoofing of the original biometric are discussed. Finally the potential impact of this technology synergy on personal privacy is considered.**

Keywords—biometrics; smartphones; personal authentication; privacy; security; zero-knowledge-proof; palmprint; iris; consumer electronics;

I. Introduction

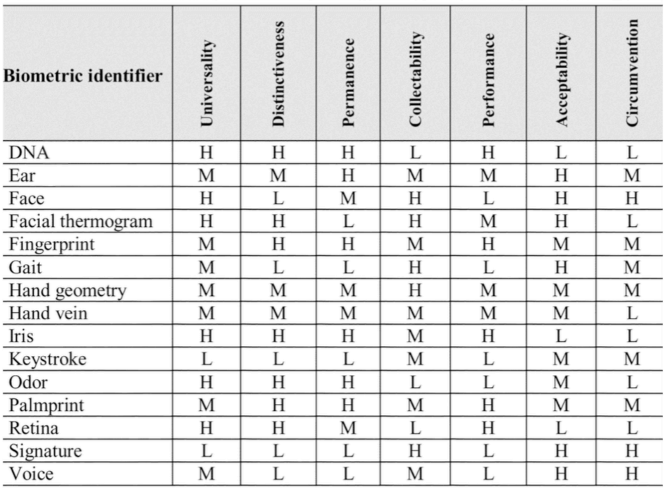
The widespread global adoption of smartphones across all demographics and the rapid commoditization of the technology to the point where an entry-level device can be sold profitably for less than 100 USD suggest that we are moving rapidly to the point where almost everyone will own a smartphone. Or, perhaps more accurately, these devices will own us! They are compelling devices, combining the capability to act as a personal messaging hub, provide mobile access to Web services, offering a sophisticated entertainment device to play music and videos and most recently a personal broadcasting engine using new Web technologies [1], should you require such capabilities. The ability of a smart-phone to augment our daily lives is already effecting 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!

Biometric systems confirm a person's identity by detecting, analyzing and then comparing patterns in physical characteristics against enrolled records of those patterns. Examples of known biometrics include scans of the face, iris or retina, geometric measures of hand geometry, 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 original use of modern biometrics is due to a French police officer, Alphonse Bertillon, who developed an anthropometric identification system for suspects in the 1880's.

The extracted patterns are matched against previously registered patterns and, within certain tolerances, a confirmed match can be used to authenticate 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.

II. Biometrics on Smartphones – an Overview

In their classic overview of Biometric Recognition Jain et al compared some of the key biometrics in terms of their key characteristics [2]:



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

Fig. 1. Key characteristics of the best known biometrics as originally presented by Jain, Ross and Prabhakar [2].

In the context of mobile handheld devices there may be some variation but it is reasonable to take these as a useful baseline for the relative merits of various biometric technologies. It is also fair to comment that this helpful chart has influenced the focus of the work presented here. For example, while iris is not the most acceptable biometric to the public, it scores high in most other metrics so a practical iris solution for mobile devices is of great interest. Likewise palmprint can be high performance and is more acceptable to the public than iris, although it is also more open to circumvention. However our main interest in palmprint is as a secondary biometric that can confirm and support authentication based on fingerprint or iris.

In the next sections we review three main biometrics that are suitable for use on smartphones and consider practical aspects of each for adoption on smartphones.

A. Fingerprint Technology and its use on Mobile Devices

Various systems to implement fingerprint biometrics have been available on handheld computers since the IPaq pocket-PC [3]–[5]. This featured a swipe fingerprint sensor and was available for several years in the early 2000's with the scanner, 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^{TM} in 2013 that fingerprint recognition really came into mainstream consumer use. The Touch ID^{TM} 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.

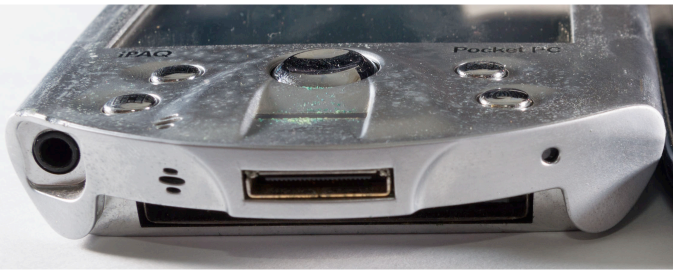


Fig. 2. A close-up of the swipe fingerprint sensor (below the main central button) on an older IPaq handheld computer.

Swipe technology was introduced due to the cost of early fingerprint scanner technology. In theory the user would swipe their finger across the scanner at an almost uniform rate and any variations would be compensated for through software post-processing. In practice, however this technique was unreliable and so early efforts to introduce consumer devices with biometric access control were unsuccessful.

In contrast Touch ID was an overnight success and by successfully blending fingerprint biometric technology into a handheld consumer device and linking the sensor to services that improved the user experience it has effected disruptive change in the consumer biometrics market [6]. The key here has been the ease of use of the technology; while it does require some effort on the part of the user the enrollment process is well managed and, most importantly, after it is completed the system works so well that the user is rarely tempted to fall back to using a PIN code. As a growing group of consumers become familiar with the technology then popular acceptance of biometrics can only become more widespread with time.

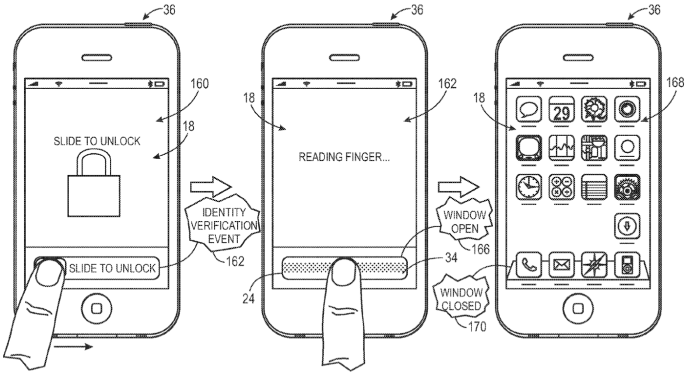


Fig. 3. Re-purposing of the finger swipe operation that is used to unlock some devices. Here the bottom region of the display is modified to sense latent fingerprints so that the swiping operation captures the finger biometric that is used to validate the user.

B. Iris Technology – How Practical is it?

The iris of the human eye has been shown to be a superior biometric [7]–[11] but is yet to make its way onto personal devices [12], [13]. In conventional systems an iris-image is acquired by a dedicated infrared imaging system and the eye is pre-aligned with the acquisition camera. In the case of a smartphone this is not practical and an unconstrained use mode is essential. In turn this poses greater challenges for the system designer.

Many systems that acquire iris-images from mobile persons are known, with the "Iris on the Move" system being one of the best known [14]. The system is proposed for airports where iris information is being used increasingly to verify passenger identity, and users are constrained to walk past a multi-camera acquisition point where multiple images are acquired under controlled illumination conditions. This differs from its use on a typical smartphone with a single fixed camera, unconstrained eye positions and limited control of illumination conditions. Some studies have begun to appear that deal directly with the iris acquisition problems for mobile phones [15]–[18] but these do not consider the current state-of-art and tend to ignore optical and quality issues that are critical for successful iris region acquisition and iris segmentation.

A detailed quality analysis of iris based systems from NIST [19] suggests that iris information is generally best obtained by illuminating the eye regions with near-infrared (NIR), which will bring out the main features of the underlying pattern. However other studies have used visible light to determine and identify iris patterns [20]–[22]. There are also studies on non-cooperative iris acquisition, typically obtained at a distance of 3-10 meters using directed NIR illumination sources [22]–[26]. In a recent paper a detailed analysis of the design problems to solve iris acquisition on current smartphones was presented [27]. This includes both optical, electronic sensor and image processing aspects.

An updated summary of the current state of progress towards unconstrained iris acquisition and authentication on smartphones is provided in a companion paper. Current research suggests that this remains a challenging problem and that a combination of specialized optical design and advanced computational imaging techniques will be required to achieve sufficient robustness and reliability to enable unconstrained acquisition.

C. *Palmprint Technology – An ideal secondary Biometric?*

Palmprint offers another alternative that is not well explored on mobile devices, but has the advantage that it does not require any additional hardware to be added to a modern smartphone. The use of palmprints as a biometric is well known in the literature [28]–[33]. However, as with other biometrics it is not trivial to adapt palmprint techniques for unconstrained use cases with mobile devices. A companion paper will present some preliminary results from such a study being undertaken in our research group and will deal with the challenges in more detail. This research is based on unconstrained acquisition where the user holds a device at a comfortable distance and simply captures a picture of their hand. Initial results are based on a database of c.20 persons and 4 devices.

The results suggest that palmprint can use existing cameras and image acquisition systems available in the current generation of commodity smartphones. This is an important factor for widespread adoption as no additional hardware costs are involved to implement these palmprint techniques. The techniques is also reasonably robust to different acquisition positions and lighting conditions.

One particular challenge is the automated extraction of the central region-of-interest (RoI) of the human palm. In the unconstrained use-case this can be acquired in an arbitrary orientation and at a variable distance from the phone camera. Several different lighting levels are also evaluated in the test database. At present the automated technique for RoI extraction achieves 95%+ success rate. Tests are also performed and verified on four different smartphone models to demonstrate consistency across devices. A number of pattern recognition techniques have been evaluated and compared with one another giving preliminary indications of the potential of this technique for practical biometric authentication on a smartphone.

Note that the primary use of palmprint is likely to be as a secondary biometric. This will be discussed later in the context of liveliness and spoofing.

D. *Other Biometrics*

There are many different biometrics and new ones are constantly being explored. Some of these require expensive hardware components (e.g. palm vein and finger vein systems) while others can require additional knowledge about the device position in relation to the user (e.g. gait measurement & analysis systems). Quite recently there was even publicity on using the touch screen of phones to obtain a geometric shape of the user's ear. Recent trends to integrate healthcare more closely on the smartphone have generated renewed interest in the use of ECG signals and pulse rates are potential biometrics.

It is clear that there is no shortage of alternative biometrics that can be sensed by our smartphones. The challenge is to consider and propose a practical infrastructure that can leverage these new inputs.

III. 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 known as verification or authentication. This 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. 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 being replaced in some countries by passports with encoded biometric data and the manual verification is replaced an electronic scan of the corresponding biometric – e.g. fingerprint, or iris codes.

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 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.

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.

Distinguishing between the willing use of biometrics by an individual to prove their identity and the covert use of this technology without a user's knowledge is important. By doing this it can be understood that most key privacy concerns are due to inappropriate and sometimes illegal use of the technology. Then a discussion can take place on the merits and benefits of the technology itself rather than becoming unduly focused on the privacy risks.

A. *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[1]. 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 every 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.

B. *Biometrics and Daily Authentication?*

If biometrics become commoditized in the near future, and this is certainly 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 [34].

But a key problem with biometrics is that they cannot be revoked. Thus if every e-mail you send has your biometric encoded into the mail signature it won't take too much effort for a cyber criminal 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 know that the iris pattern can be reverse engineered from a simple binary iris code [35].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. But 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.

C. *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 smart-phones 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?

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?

Well it doesn't take a rocket scientist to realize that our 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!

D. *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

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

same authentication code(s). But there is another layer of security here, because your device stores your authentication code in a secure memory and never exports it. Instead it uses a well-known cryptographic technique known as *zero-knowledge-proof* (ZKP) to authenticate you to a network based service where you are enrolled [36]–[38]. 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 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 become 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.

IV. Biometrics, Security and Identity Theft

In the earlier sectons we discussed the use of biometrics as a means of personal authentication. Naturally the next concern stems from this use – if my biometrics can 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 a long 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.

A. *Potential Spoofing of the Biometric*

It is almost impossible to have a conversation about biometrics without the mention of the potential to ‘spoof’ a person’s biometric. It is a fair and valid criticism, yet many current systems make use of immutable data to verify a person’s identity. As an everyday example, your date of birth is frequently used as a crosscheck on your identity. It is one of the most common questions when setting up, or verifying a bank account by telephone or when resetting your bank password when you’ve forgotten it. Your date of birth does not change, so how is this different from a biometric?

Nevertheless 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 [39] to modify the iris patterns in any faces detected by an imaging device. This is not as far fetched as it might seem - many modern imaging devices incorporate real-time face tracking technology that enables to follow faces throughout an imaged scene.

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 if playback is at high frame rates, 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 recognition rates. Daugman has published results of studies involving the order of hundreds of billions of cross-comparisons of iris codes [11] 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. A LED light source can provide a secondary liveness detection that verifies the facial region by detecting an active glint in the pupil of the eye to show it if is a live eye and confirming that the face and lips regions are also live.

B. *The Risk of Data & Identity Theft*

Now if my biometrics can 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 a long time and one that can be largely addressed by *liveness detection* (discussed above). Thus while it is possible to capture a video of my face and eyes and potentially show a high-resolution video to a device it is relatively straightforward to shine a light on the false face and determine that the pupil does not provide a correct glint response.

More sophisticated technique involve the use of iris patterns embedded into a contact lens [12], [40], [41]. While this appears to be a very sophisticated approach on further consideration one realizes that only very specialized companies can manufacture such high quality contact lenses without give-away manufacturing patterns embedded into the lens, and as there are less than a handful of such companies world-wide and they are required to keep detailed records it is very difficult to see how a cyber-attacker might proceed without leaving a very obvious logistical trail. In any event sophisticated detection approaches have been developed even for advanced contact lens technology [42]–[44].

And so while identity theft via stolen biometrics is possible, it is not trivial. And the challenges posed are only likely to grow more sophisticated in the future. Thus, for those who wish to engage in such activity, conventional pen and paper identity theft is definitely going to be a lot more straightforward than the biometric variety.

C. *Supervised Vs Unsupervised Authentication*

This is perhaps the biggest leap with smartphone biometrics – almost all 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 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^{TM} 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, as mentioned elsewhere, 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 cutomer 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 unless they manage to lose it and then they can get to a network and hit the kill switch!

V. Biometrics and 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 [45] has written in detail on this topic. He separates privacy into quite a few sub-aspects and emphasizes the need for various 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 the worst fears expressed in popular culture may well become reality. Naturally, as per earlier discussions, it is not envisaged that smartphones will become harvesting devices for your personal biometrics – instead they should be considered as preventing this centralized harvesting. If your device can authenticate you reliably, why should your biometrics be available beyond your device?

Jain and Nandakumar [46] 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: (i)

- "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.

The use of biometric technologies in this context needs to be addressed carefully, but if applied thoughtfully it has potential to solve problems rather than create them. In the context of consumer systems and products – if adopting biometric technologies makes our lives simpler and more manageable it seems a difficult proposition to argue against, especially if a smartphone is used to curate the personal data, protect its integrity and act as an honest broker between the user and cyberspace. After all we do love our smartphones, and they do make our lives easier in many respects. How long until we come to trust them too?

ACKNOWLEDGMENT

The research work presented here was funded under the *Strategic Partnership Program* of Science Foundation Ireland (SFI) and co-funded by SFI and FotoNation Ltd. Project ID: 13/SPP/I2868 on *Next Generation Imaging for Smartphone and Embedded Platforms.*

REFERENCES

[1] A. Rutkin, "Smartphone spectators," *New Sci.*, 2015 [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0262407915301135. [Accessed: 29-May-2015]

[2] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, 2004.

[3] W. Jansen, "Authenticating users on handheld devices," *Proc. Can. Inf. Technol. ...*, 2003 [Online]. Available: http://csrc.nist.gov/groups/SNS/mobile_security/documents/mobile_devices/PP-AuthenticatingUsersOnPDAs.pdf. [Accessed: 29-May-2015]

[4] 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 [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4146036. [Accessed: 07-Jan-2012]

[5] 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 [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4588002. [Accessed: 07-Jan-2012]

[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 [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0969476514700888. [Accessed: 29-May-2015]

[7] A. K. Jain, A. Ross, and K. Nandakumar, "An introduction to biometrics," *2008 19th Int. Conf. Pattern Recognit.*, 2008.

[8] K. W. Bowyer, "Iris Recognition : From Basics to Research Frontiers," *Iris Recognit. Tutor. BTAS 2013*, 2013.

[9] J. G. Daugman, "Biometric personal identification system based on iris analysis." Google Patents, Mar-1994.

[10] J. Daugman, "The importance of being random: Statistical principles of iris recognition," *Pattern Recognit.*, vol. 36, pp. 279–291, 2003.

[11] J. Daugman, "Probing the Uniqueness and Randomness of IrisCodes: Results From 200 Billion Iris Pair Comparisons," *Proc. IEEE*, vol. 94, 2006.

[12] K. W. Bowyer, K. Hollingsworth, and P. J. Flynn, "Image understanding for iris biometrics: A survey," *Comput. Vis. Image Underst.*, vol. 110, pp. 281–307, 2008.

[13] J. Daugman, "How Iris Recognition Works," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 21–30, Jan. 2004.

[14] J. R. Matey, O. Naroditsky, K. Hanna, R. Kolczynski, D. J. LoIacono, S. Mangru, M. Tinker, T. M. Zappia, and W. Y. Zhao, "Iris on the Move: Acquisition of Images for Iris Recognition in Less Constrained Environments," *Proc. IEEE*, vol. 94, 2006.

[15] D. Jeong, H. Park, K. Park, and J. Kim, "Iris recognition in mobile phone based on adaptive Gabor filter," *Adv. Biometrics*, 2005 [Online]. Available: http://link.springer.com/chapter/10.1007/11608288_61. [Accessed: 21-May-2014]

[16] D. Cho, K. Park, and D. Rhee, "Pupil and iris localization for iris recognition in mobile phones," *Softw. Eng. Artif. Intell. Networking, Parallel/Distributed Comput. 2006. SNPD 2006. Seventh ACIS Int. Conf.*, pp. 197–201, 2006 [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1640689. [Accessed: 21-May-2014]

[17] K. Park, H.-A. Park, B. Kang, E. Lee, and D. Jeong, "A Study on Iris Localization and Recognition on Mobile Phones," *EURASIP J. Adv. Signal Process.*, vol. 2008, no. 1, p. 281943, 2008.

[18] S. Kurkovsky, "Experiments with simple iris recognition for mobile phones," in *Information Technology: New Generations (ITNG), 2010 Seventh International Conference on*, 2010, pp. 1293–1294 [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5501569. [Accessed: 21-May-2014]

[19] E. Tabassi, P. Grother, and W. Salamon., "IREX II - Iris Quality Calibration and Evaluation (IQCE): Performance of Iris Image Quality Assessment Algorithms.," 2011 [Online]. Available: http://biometrics.nist.gov/cs_links/iris/irexVI/irex_report.pdf. [Accessed: 21-Mar-2014]

[20] H. Proenca and L. A. Alexandre, "Iris Recognition: Measuring Feature's Quality for the Feature Selection in Unconstrained Image Capture Environments," *2006 IEEE Int. Conf. Comput. Intell. Homel. Secur. Pers. Saf.*, 2006.

[21] H. Proenca, "Iris Recognition: A Method to Segment Visible Wavelength Iris Images Acquired On-the-Move and At-a-Distance," in *Advances In Visual Computing, Pt I, Proceedings*, vol. 5358, 2008, pp. 731–742 [Online]. Available: <Go to ISI>://WOS:000264057800070

[22] H. Proenca, "On the feasibility of the visible wavelength, at-a-distance and on-the-move iris recognition," *2009 IEEE Work. Comput. Intell. Biometrics Theory, Algorithms, Appl.*, 2009.

[23] T. Tan, Z. He, and Z. Sun, "Efficient and robust segmentation of noisy iris images for non-cooperative iris recognition," *Image Vis. Comput.*, vol. 28, pp. 223–230, 2010.

[24] Y. Du and E. Arslanturk, "Video based non-cooperative iris segmentation," in *Mobile Multimedia/Image Processing, Security, And Applications 2008*, 2008, vol. 6982, p. 69820Q–69820Q–10 [Online]. Available: http://proceedings.spiedigitallibrary.org/proceeding.aspx?articleid=1332985

[25] K. Yang and E. Y. Du, "A multi-stage approach for non-cooperative iris recognition," *2011 IEEE Int. Conf. Syst. Man, Cybern.*, pp. 3386–3391, 2011.

[26] J. M. Colores, M. Garcia-Vazquez, A. Ramirez-Acosta, and H. Perez-Meana, "Iris Image Evaluation for Non-cooperative Biometric Iris Recognition System," in *Advances In Soft Computing, Pt Ii*, vol. 7095, 2011, pp. 499–509 [Online]. Available: <Go to ISI>://WOS:000308845000044

[27] P. Corcoran, P. Bigioi, and S. Thavalengal, "Feasibility and Design Considerations for an Iris Acquisition System for Smartphones," in *2014 IEEE Fourth International Conference on Consumer Electronics - Berlin (ICCE-Berlin) (2014 IEEE ICCE-Berlin)*, 2014.

[28] A. Kumar, D. Wong, H. Shen, and A. Jain, "Personal verification using palmprint and hand geometry biometric," *... -and Video-Based Biometric ...*, 2003 [Online]. Available: http://link.springer.com/chapter/10.1007/3-540-44887-X_78. [Accessed: 29-May-2015]

[29] D. Zhang, *Palmprint authentication*. 2004 [Online]. Available: https://books.google.com/books?hl=en&lr=&id=4tdShJALfA0C&oi=fnd&pg=PR9&dq=palmprint+authentication&ots=osrfRq43_4&sig=irjNKKKeE0F2ZwIMPnBmhYDoaaE. [Accessed: 29-May-2015]

[30] A. Kong, D. Zhang, and M. Kamel, "A survey of palmprint recognition," *Pattern Recognit.*, 2009 [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0031320309000399. [Accessed: 29-May-2015]

[31] A. Morales, M. Ferrer, and A. Kumar, "Improved palmprint authentication using contactless imaging," *... Theory Appl. ...*, 2010 [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5634472. [Accessed: 29-May-2015]

[32] D. Zhang, W. Zuo, and F. Yue, "A comparative study of palmprint recognition algorithms," *ACM Comput. Surv.*, 2012 [Online]. Available: http://dl.acm.org/citation.cfm?id=2071391. [Accessed: 29-May-2015]

[33] N. Duta, "A survey of biometric technology based on hand shape," *Pattern Recognit.*, 2009 [Online]. Available:

http://www.sciencedirect.com/science/article/pii/S0031320309000752. [Accessed: 29-May-2015]

[34] 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 [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6227433. [Accessed: 15-Aug-2013]

[35] 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.

[36] 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.

[37] 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 [Online]. Available: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=6031855. [Accessed: 19-Jan-2012]

[38] 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 [Online]. Available: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=6018903. [Accessed: 19-Jan-2012]

[39] S. Thavalengal, R. Vranceanu, R. G. Condorovici, and P. Corcoran, “Iris Pattern Obfuscation in Digital Images,” in *International Joint Conference on Biometrics*, 2014, p. In Press.

[40] C. Roberts, “Biometric attack vectors and defences,” *Comput. Secur.*, vol. 26, no. 1, pp. 14–25, 2007.

[41] A. Hadid, “Face Biometrics under Spoofing Attacks: Vulnerabilities, Countermeasures, Open Issues and Research Directions,” in *CVPR*, 2014, no. Cmv, pp. 113–118.

[42] S. E. Baker, A. Hentz, K. W. Bowyer, and P. J. Flynn, “Contact lenses: Handle with care for iris recognition,” in *IEEE 3rd International Conference on Biometrics: Theory, Applications and Systems, BTAS 2009*, 2009.

[43] N. B. Puhan, S. Natarajan, and A. Suhas Hegde, “Iris liveness detection for semi-transparent contact lens spoofing,” in *Communications in Computer and Information Science*, 2011, vol. 205 CCIS, pp. 249–256.

[44] K. Hughes and K. W. Bowyer, “Detection of contact-lens-based iris biometric spoofs using stereo imaging,” in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2013, pp. 1763–1772.

[45] R. Clarke, “Biometrics and privacy,” *Retrieved Novemb.*, 2001 [Online]. Available: http://www.rogerclarke.com/DV/Biometrics.html. [Accessed: 29-May-2015]

[46] 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 [Online]. Available: http://www.computer.org/csdl/mags/co/2012/11/mco2012110087.html. [Accessed: 05-Sep-2013]