Hazards of Biometric Authentication in Practice

Samantha S. S. Phang
Commonwealth Bank of Australia
Digital Protection Group
Sydney, NSW, Australia

Christopher J. Pavlovski
Commonwealth Bank of Australia
Digital Protection Group
Sydney, NSW, Australia

***Abstract*—With the increase in cyber threats and attacks many institutions are exploring how newer technologies may be applied to strengthen the way users are verified when bestowing permissions for carrying out web transactions. In particular, many institutions are under increasing pressure to improve the security instruments used to authenticate users, while permitting access to their personal records to approve transactions. Whilst multifactor authentication protocols have been adopted to validate more sensitive transactions, this has added an additional physical interaction during the verification process. More recently, the industry has turned its attention to the use of biometric authentication as a way to securely verify user identities. This has reduced the complexity associated with existing authentication processes that require passwords, tokens, and challenge-response keywords. This paper explores these new authentication techniques, discussing the benefits while highlighting the challenges in practice to using biometrics. In particular, identity theft of biometric markers and its potential impact to customers and liability challenges for institutions are presented.**

***Keywords*—biometric authentication; cyber threat; identity theft**

I. Introduction

As newer digital technologies evolve to become available for use in industry applications the opportunity exists to improve the way customer interact with on-line systems while strengthening security and improving ease of use. Biometric authentication is one such technology which has been regarding as an advanced tool to improve the strength of the verification process of users but also improve the usability aspects by simplifying the authentication process for people. Whilst a range of biometric technologies have been in use for some time for several authentication systems, such as access to restricted areas or sensitive (secret) facilities, it has recently gained attention as a technology option for mainstream industry. In particular, it has been suggested as a practical way to strengthen and improve the authentication of on-line customer wishing to conduct personal and sensitive transactions.

Cyber threats have continued to increase in volume and complexity and in some cases exponential growth has been experienced in certain types of attack. The traditional means for authenticating users has often relied heavily upon the username and password credential. This has often been strengthened with digital certificates, secure hardware tokens, or the addition of multiple authentication challenges; as seen in multi-factor authentication. There are several drawbacks to these existing systems which have seen cyber attackers successfully obtained credentials of the users. For instance, one study estimated that 50% of users reuse their passwords [1]; it follows that the attacker need only compromise one (less secure) site to gain credentials for other potentially more sensitive online accounts for the same user. Hence, there are motivations for institutions to explore alternative and stronger forms of authentication to counter these cyber threats. In particular, biometric authentication has emerged as a strong candidate to fulfil this need.

In this paper, the industry application of biometric authentication is critically examined. The most recent innovations to apply this form of authentication are assessed to understand the benefits these new technologies bring and also the potential challenges that may arise. Given that the security protocols involve the use of the most sensitive human personal data, biometric information, there is particular importance to understand what risks may be encountered when applying such tools in practice. Hence, the main contributions of this paper include the following.

- The industry applications of biometric authentication and the projected trends for use are assessed;
- Analysis is conducted of the industry challenges in practice with the use of human biometric markers; and
- The potential consequences and liabilities to people and institutions are assessed.

In the next section a review of the literature related to biometric authentication is discussed. Section three discusses the set of human biometric identifiers that have been considered as tools in building or enhancing authentication systems. In section four, several applications that have been proposed for the industry in practice are explored. This is followed by section five where the challenges and risks to using biometric markers are evaluated with the risks and liabilities for both the customer and business, in particular the implications to the industry in the event of a data breach is examined. The paper is concluded in section six with a discussion of the key observations made in the paper while several areas of further work are presented.

II. Related Work

There has been a great deal of work related to the use of biometrics for authentication purposes. Much of that work has focused on applying a variety of biometric identifiers to strengthen the existing authentication protocols and schemes.

ISSN (Print): 2204-0595
ISSN (Online): 2203-173

While an adopted form of biometric authentication is its use in border security, one study on the use of facial recognition suggests that this is inadequate in large applications such as border control [2]. Multimodal biometric schemes have also been proposed for border control applications that utilize facial recognition together with fingerprinting on e-passports [3]. Further works suggests the use of multi-modal biometric schemes can also be used to overcome some of the limitations of using single biometric identifiers in authentication [4].

Two factor authentication systems have also been proposed as an approach for strengthening traditional username password credential based systems. The use of a biometric marker (voice) together with an additional (non-biometric) authentication factor was analyzed in [5]; the authors conclude that the second factor may not contribute to strengthen the overall protocol. Combining biometrics with mobile technology has also been studied together with a username password authentication factor [6]. The paper examines the use of facial, voice, and gestures, revealing issues in usability and performance, in particular noting that facial and voice are not universally usable. A further study reported an alternative view in which biometrics are considered more usable in comparison to passwords on a mobile device [7]. Several additional approaches to using biometrics have also been investigated, such as biometrics authentication as a service for enterprise identity management [8], approaches to using biometrics in authentication in ad-hoc networks without the presence of an authentication server [9], and augmenting traditional web applications with a voice biometric authentication capability to improve confidence in the customer identity and reduce transaction fraud [10].

Finally, we observe the literature related to understanding the risk and challenges of using biometric [11–13]. In [11], the authors disclose biometric uses and corresponding security and privacy issues of using these, suggesting that biometrics does indeed raise several privacy concerns and that a sound trade-off between security and privacy may be necessary. A further investigation of issues concerning biometric profiling is presented in [12], where it is observed that biometrics may be used as a source for profiling information with the risks including loss of control over personal data, concerns in discrimination, and legal implication. Schneier remarks that while biometric identifiers are difficult to forge they are easy to steal [13]. Moreover, he observes that biometric data are unique identifiers but are not secrets; once it is stolen there is no mechanism to revoke the identifier, it is effectively stolen for life [13].

The work herein may be considered an extension of this particular focus area of risk, as an in-depth assessment of the risks and challenges are covered for institutions and people. In particular, noting the potential harm that may be caused (the human aspect), which in turn will ultimately lead to financial and legal liabilities for institutions, whether this is due to an institutional data breach or the universal ability to covertly steal biometric marker from people.

III. Biometric Authentication Markers

Biometric identifiers for authentication purposes are generally derived from two categories: i) physiology or ii) behavioral human traits. Physiological traits as biometric identifiers are related to the shape of body parts. This includes fingerprints, hand geometry, palm print, facial appearance, iris pattern, retina pattern and human DNA. Conversely, voice, pulse rate, body heat signature, gait, keystroke dynamic, and hand signature (pen pressure and signature speed) are biometric identifiers related to pattern of a person's behavior. We now discuss in more detail some of the more commonly applied traits for these two categories.

A. *Physiological Biometric Identifiers*

The fingerprint is uniquely identified by a pattern of ridges and valleys, known as minutiae features, on the surface of the fingertip. The fingerprint of each finger is different and is unique for each individual, including identical twin. Fingerprint formation is fully developed during the first seven months of fetal development. The pattern remains stable over a person's lifetime with exception of damage caused by external factors such as injury or disease. The distinct features of the fingerprint are segmented and extracted through advanced image processing techniques after the live scan. Correlation-based matching and pattern-based (ridges or valleys) matching are the common fingerprint identification techniques used.

Hand geometry is a biometric that identifies an individual by the shape, size of palm, length and width of fingers of the hand. Standard optical camera or flat-bed scanners are common devices used to capture hand images in hand geometry recognition systems. In many cases finger position guides are used to ensure consistency of hand image capture. The key features of the person hand are extracted from the black and white silhouette of the digitized grey scale hand image. Some of the common matching approaches used include Euclidean distance metrics, correlation method and principal component analysis [14].

The iris is composed of a random texture pattern within the human eye and is unique for each individual including identical twin. Iris patterns on the left and right eyes are also different. The iris pattern stabilizes within the first 2 years of life and remains unchanged unless there is damage due to eye disease (e.g. cataract) or unsuccessfully eye surgery. A common approach for iris recognition systems is to apply near infrared light to acquire iris images. This is more effective in revealing rich texture for dark brown eyes compared to light colored eyes. The iris code can be generated in one dimension using normalization resolution levels of iris features, or two dimensions using techniques such as Gabor filters [15] and Laplacian pyramid [16]. The Hamming distance [17] and Fisher discriminant [18] are some of the well-known matching approaches used to measure the similarity of two irises. A related biometric is the retina scan which involves detects the patterns of veins in the back of the eye to accomplish recognition.

Palm-print recognition measures the inner surface of the hand. The process obtains geometric features (i.e. palm shape), minutiae features, principal lines, wrinkles and delta point

ISSN (Print): 2204-0595
ISSN (Online): 2203-173

features that are unique to the individual. Identical twins have enough distinctive palm-print features for recognition purposes. Given the richness and breadth of palm-print features, it is considered a more accurate biometric identifier compared to hand geometry and fingerprints. Methods used to represent palm-prints can be divided into five categories [19], these are: i) line-based, ii) appearance-based, iii) local statistic based, iv) global statistic based, and v) coding based. In addition to the fingerprint and hand geometry matching algorithms, the Hamming distance approach is also commonly used to match two palm-prints.

Facial recognition involves identification based upon the attributes of a person face. Recognition data is extracted in either two or three dimensional facial images. There are two broad categories to face recognition approaches. Feature-based, which uses properties and geometric (e.g. areas, distances and angles) relations of between facial features as recognition descriptors. The second is an appearance-based method which involves an analysis of the face image intensity pattern. Some of the popular matching algorithms used include Principal component analysis, Linear Discriminant Analysis and Tensor faces, Manifold Learning method, and Kernel method [20].

Deoxyribonucleic acid (DNA) is classified as a chemical biometric. This marker may be used for authentication and the identification of an individual is achieved through the analysis of partial segments of the DNA strand.

B. *Behavioural Biometric Identifiers*

Voice as an authenticator may be applied with a combination of acoustic and behavioral patterns. The acoustic patterns are influenced by the shape and size of vocal tracts, mouth, and nasal cavities, while the behavioral patterns are defined by voice pitch, speaking style, and sociolinguistic trait. The acoustic patterns are more stable than behavioral patterns over time due to age, medical conditions, and emotional state. The key features extracted from a person voice forms the voice print used for authentication. Template matching and feature analysis are two widely used voice recognition approaches. The goal of matching is used to find similarities between the stored and the actual voice print. Template matching involves detection of a near-exact match between a previously stored voice print and the voice print to be authenticated. For feature analysis, voice data for matching is processed using statically models like Fourier transformations, hidden Markov models or Gaussian mixture models to generate the voice print. Text-dependent and text-independent are two types of commercially used voice recognition systems. The matching of the former system is based on utterance of fixed predetermined phrase for enrollment and for verification, whilst there is no constraint on the speech content for the latter in the matching process.

Hand written signatures are a behavioral characteristic of a person signing their name. Signature recognition can be operated in off-line or on-line manner. Off-line analysis detects the similarity of the signature shape for two digitized static signature images. On-line mode refers to acquiring signature in real time using acquisition devices like touch screens or digitizing tablets and capturing dynamic features like position trajectories, timing, pressure, speed of signing and size of signature; which are very difficult to mimic. Individuals must sign their name multiple times during an enrolment process. Enrolment can be divided into reference-based and model-based approaches depending on the matching strategy. In reference based systems a set of signature templates are generated, with the features extracted from the set of enrolled data. While a model-based system involves a statistical model which describes the behavior of the signor which is estimated from the enrolled data. Popular matching techniques applied for signature recognition are dynamic time warping, hidden Markov models and vector quantization [21].

Gait recognition is the identification of a person based on the manner in which they walk. This can be used to from a distance which make this trait suitable appropriate in surveillance applications. Model based gait recognition techniques involve extraction of spatial-temporal attributes of a moving individual. This is derived from the silhouette or optical flow associated with a set of dynamically moving points of the moving human body and used to describe the gait of an individual. Approaches that recognize individual through binary gait silhouette sequence belong to appearance-based approaches.

Keystroke dynamic is determined by how a person types on a keyboard and is based upon habitual typing rhythmic patterns. While this trait is not as unique as other biometric traits, the minor variation is said to offer sufficient discriminatory information to identify a person. Some of the common keystroke recognition techniques include static at login which observes typing pattern using a known keyword or phrase, periodic dynamic that analyses the typing pattern characteristic over a specific timeframe, and continuous dynamic which monitors the typing behavior during a series of interactions. Other techniques include keyword-specific, achieved by continuously monitoring the typing pattern for specific set of keywords and digraph latency which measures the time between the key-up and next key-down action.

IV. Biometric Applications in Practice

In the past, the application of biometric technology has predominantly been used for forensic purposes such as fingerprint collection at a crime scene or determining heritage via DNA matching. The adoption of biometric technology to solve other business problems has increased as the technology has matured. These solutions can be generally categorized into commercial and government applications. The government applications may include national identification cards, driving licenses, and passports. These have subsequently been extended for use in border control, passport control and welfare-disbursement. For example, recent border control systems allow travelers to use a kiosk then pass through a facial recognition system that is compared with the image stored on an e-passport microchip to verify the person.

Some governments have adopted Iris recognition technology for social benefit claim, while humanitarian organizations use this for aid distribution control to manage aid entitlement for people. More recently, Amber Alert, a face recognition technology, has been launched by government agencies in various countries and social media company to find missing persons [22, 23]. In some countries biometric technology is used to prevent voter fraud. The Mobile Offender Recognition and Information System (MORIS) has been developed for police officers to scan biometrics and retrieve any criminal history of a subject in near real time [24]. Surveillance monitoring is another application where law enforcement authorities apply facial identification technology to identify criminal in the live surveillance streaming at airport. This type of application is also common in places such as Casinos to identify and alert relevant staff to the presence of blacklisted or high risk customers.

The commercial applications of biometric technology are more extensive. The applications include wireless authentication, device security authentication, logical access control, physical access control, negative recognition, time and attendance, and transactional authentication. Laptops and notebooks are now built with biometric scanning devices that enable a user to quickly logon. Additionally, many smart phones are equipped with cameras and biometric scanning tools for authentication. These ideas have unlocked a range of network, online and mobile applications to include biometric as an alternative authentication method. For instance, there are a number of Android applications that employ facial recognition to ensure the application is only accessible by the purchaser or selected user. There are also applications available that allow the user to encrypt their document using their hand written signature or to generate cryptographic keys based on time functions of their hand written signatures.

Banking, telecommunications, and the health sector are the few major industries that use biometrics for granting controlled logical access. The solutions rely upon the native biometric capability built into smartphones and notebooks and enable customers to access their financial and phone accounts. Some financial institutions use passive speaker recognition to verify telephone customers [25], while telecommunications carriers have adopted voice recognition to identify telephone customers, with the aim to reduce the operational cost of the call center. The media industry uses voice biometrics to control access to media content for media authors, producers, and final users. In the health industry, biometric systems are used by medical staff and patients to access patient electronic medical records. Furthermore, some hospitals leverage hand vascular systems in their medical supply dispensation systems to ensure that restricted and expensive drugs are not stolen.

Biometric authentication for physical access control has been widely used by the sporting and entertainment industry. For example, controlling access to the Atlanta Olympic Village was accomplished with the fingerprints of athletes, staff and volunteers. The approach has been also used to manage paid physical access where subject's biometrics are used as the ticket or pass. One motivation for theme park venues was to prevent visitors buying unused ticket or partially used tickets from others. Biometrics is often used to gain access to highly sensitive restricted premises, such as access company data center or a hospital operating room. Physical access control has also widely been used in the government sector to control highly restricted and sensitive premises such as nuclear plants. Many government agencies have deployed biometric systems in many sensitive and public areas for close monitoring and negative recognition (i.e. prevent a single person from using multiple identities by establishing whether the person is who that person implicitly or explicitly denies being). Banks also use biometrics as negative recognition to prevent lawbreaker from creating new accounts or lines of credit.

Biometrics based time and attendance terminals are becoming increasingly popular in many industries to ensure that employees cannot *clock-in* for one another, thereby preventing employee time theft. This concept has also been adopted in the education industry to track accurate student attendance, and in distance learning to ensure students actually attended the minimum number of hours for online lectures. Many banks have deployed biometric based Automatic Teller Machines to prevent fraudulent withdrawals using fake, lost or stolen credit cards. In the U.S, some retail stores have deployed biometric systems to help customer cash their pay-checks or make a payment after a purchase.

V. Adoption Challenges and Liabilities

In this section some of the challenges of adopting biometric authentication in practice are presented. Invariably many of these challenges may be addressed with improvements in sensory technology. However, biometric identity theft presents a difficult challenge to industry and is likely to compound as biometrics adoption becomes more widespread. Moreover, an analysis is presented of the potential liabilities that institutions may incur due to biometric data breaches and general biometric identify theft from individual due to malicious surveillance.

A. General Challenges in Practice

While the matching accuracy of fingerprints to identify a person is relatively high, fingerprint recognition still faces challenges with the poor quality of acquired data due to several issues. This includes large pixel displacement of fingerprints (resulting from different finger location on the sensor during acquisition), non-linear distortion of converting three dimensional objects to two dimensional images, and differences in pressure applied on the sensor and varying skin conditions of the finger. The sensor technologies available belong to optical, ultrasound or solid-state (capacitive, thermal, electric field, piezoelectric) families [26]. Additional problems occur with the formation of scar tissue and dirt upon the fingertips. Fingerprint residues are left almost everywhere by people making them extremely vulnerable to illegal capture.

In general, hand geometry is not very distinctive trait as one in every 100 people have very similar hand features to another person, hence this identifier is not suitable for identification of an individual when drawn from large population size. Similar to the fingerprints, humans leave residue of the hands constantly and hence the ability to capture hand geometry is straightforward for a threat actor. Hand geometry varies across a persons' age due to physiological changes of the person (e.g. physical growth or weight gain). Template adaptation techniques that adapt the hand geometry to the individual's physiology changes over time and has shown to improve matching performance [14]. The advantage of this identifier is that factors like weather or individual anomalies do not affect the accuracy of recognition. However, obstructions such as

ISSN (Print): 2204-0595
ISSN (Online): 2203-173

rings, dirt, and large bandages could affect the matching performance. Conversely, palm-print recognition faces both challenges of physical changes over time and external obstructions that hinder the performance of the system.

The matching performance of commercially available facial recognition systems are constrained due to factors such as facial poses, camera view points, ageing, makeup, and eyeglass. In particular, illumination and expressions conditions have been the focus of face recognition research. Computer vision approaches such as Active Appearance Models and Elastic Bunch Graph Matching have been shown to improve the recognition performance for facial images with different poses and facial expression [27].

The accuracy and the speed of iris recognition is very high. The iris system has very low False Acceptance Rate (FAR), but rather has a high False Rejection Rate (FRR) compared to other biometric traits [28]. The major challenge of iris recognition is the hippus movement of pupil due to changes in lighting condition. While this movement is used to measure the liveliness of the iris, it distorts the iris pattern which result in high FRR when performing matches against it. Although techniques can be used to restore the iris pattern to desired pupil size [29]. Other major problems include poor quality of iris images acquired due to eyelid, eyelashes, and reflections hindering the iris features extraction.

While DNA is a very distinctive trait the key challenge in the adoption of DNA based biometric system has been due to the debate regarding its potential for misuse and this being generally intrusive; (i.e. human profiling, and health status, and ethics).

The human voice pattern not a very distinctive identifier and the accuracy of voice recognition systems in authentication are affected by changes in behavioral patterns of the voice, background noise and differences in the devices used between enrolment and voice recognition stage.

The gait of a person can be modified by many factors which changes the normal locomotive traits, in some cases permanently. The factors include extrinsic such as footwear and clothing, intrinsic such as age, and physical attributes such as weight & height. In addition, pathological insults can also influence a persons' gait; this includes trauma, musculoskeletal anomalies, and psychiatric disorders.

Hand related behavioral biometrics such as keystroke dynamic and signatures are not common. Factors like emotional state, type of keyboard used and its position with respect to the person could vary the person's typing pattern. While the key disadvantages of hand signature recognition are the large intra-class variation and the behavior is influenced by physical and emotional conditions.

B. *Privacy Implictions of Biometric Authentication*

While many early adopters of biometric technology see the benefits in improving cost-effectiveness, improved efficiency, and better customer service, this technology may well have implications on human rights and privacy issues for those who take part. Biometric data is mostly collected along with the personal identifiable information of an individual. However, when an organization collects data for one purpose and decides to apply this for another purpose, without the person's consent, they are likely to be ethical and liable ramifications. For instance, a recent lawsuit on facial recognition software is a classic example where users sued an organization for violating their privacy by identifying and tagging them in photos without their consent [30].

Another privacy challenge is the covert collection of an individual's biometric without a person's knowledge, and the subsequent masquerade and use without consent. The human face may now be captured in a very straightforward manner, without the person being aware. This is more simplistic with the era of social media where facial images or video can be downloaded from a persons' social media site. Similarly, fingerprint can be easily obtained from latent prints on any touched surface.

Many biometrics, especially behavioral biometrics, could reveal secondary information about an individual. This may include general health disposition, the likely occupation, and social economic status. In some cases, the secondary information may be used to place those individuals at a disadvantage. The majority of the biometric data captured and stored are unregulated and there are very few regions that have biometrics information privacy acts to protect the public from misuse. Moreover, there is no law (to date) that restricts others from collecting biometric data without a person's knowledge. While the regulatory constraints are not in place the prospect of human biometric data being used beyond what is initially consented to is very high.

When a personal identity is stolen today, one may ultimately resort to changing their name. Given the intrinsic properties of biometric identity to an individual, the ability to change this identifier will no longer be available – once stolen the person is impacted for the remainder of life and all authentication systems that rely upon this data are effectively compromised. Not only is it relatively easy to obtain raw biometric data of a person in public, many biometric systems in place have flaws in protecting both the biometric data and personal identifiable information stored. For example, security flaws are noted in an e-passport system [31], where attackers can access the RFID in the passport, which contains digitally signed biometric information, wirelessly without the passport's holder knowledge.

If the digitized biometric data is not encrypted either at rest or in transit, it will be subjected to man-in-the-middle (interception) attacks. Furthermore, if an institution trusts a new biometric system beyond appropriate levels, then they run the risk of assuming identities and transactions are legitimate when they may not be. Moreover, they may initially place the onus on the customer to show that a transaction is fraudulent, rather than the institution demonstrating that the transaction was legitimate. If an imposter can spoof a biometric characteristic, perhaps by creating a false finger, they may be able to enroll or use a service without having to produce the traditional identity documents that would normally be required.

C. *Biometric Identiy Theft: The Liabilities*

The most obvious challenge with the use of biometric markers for authentication is the propensity of these markers to be easily stolen. Human biometric markers are generally visible to everyone with people leaving physical residues on everything we touch, everywhere we go. Hence, many traits can be obtained in a generally straightforward manner using commodity technology available in the marketplace. Moreover, camera technology is sufficiently mature to enable high resolution photography of facial features, geometric attributes, and observable characteristics. For example, researchers from Carnegie Mellon University have recently made covert collection of iris scans, one of the most difficult biometric markers to acquire, in good quality without the persons' cooperation; this has been achieved from a distance of 12 meters from the target individual [32]. The most important implication of this theft, as pointed out by Schneier [13], is that once the biometric marker is stolen "it is stolen for life" and can no longer be used again. Conversely, when a password is stolen, this can be changed.

In general, there are two common biometric identity theft scenarios: i) data breaches sustained by an organization and ii) the general theft of biometric markers from illegitimate surveillance by a threat actor. Moreover, where an institution provides a biometric authentication capability to users without an alternative authentication option, (i.e. the user has no choice but to use it), it is likely that the institution is also liable for the compromise of any customer account from biometric theft, due to the ease of which biometric markers may be stolen. Furthermore, once they are stolen, the institution will ultimately require an alternative form of authentication, since it is not possible to change biometric markers as one would easily change a lost or stolen password.

The potential consequences to an organization include detrimental impact to corporate brand, loss of reputational status, and erosion of trust within the marketplace. Further, there are likely to be regulatory penalties imposed by authorizes on any data breach that pertains to biometric data. There is also the likelihood of class action legal pursuit from the aggrieved customers for compensation. Furthermore, the potential for additional financial impact from competing or partner organizations exists. A company which sustains a data breach of customers' biometric data may also be liable to pay for the losses (and other maintenance costs) of other companies which uses the same biometric data of compromised customers.

VI. Discussion and Conclusions

There are several motivations to apply biometrics markers for authentication purposes to the industry. This includes ease of use for customers, cost-effective solution alternative, and relative fast and efficient means of user authentication. The application of these emerging techniques can also be viewed by the industry as being market leading for the institution adopting such technologies. While these benefits may be appealing there are several key challenges facing the use of biometrics markers that have been discussed. Many of the challenges are technical obstacles in ensuring the authentication technologies function as intended. However, the key challenge and implications of biometric identity theft require much deeper consideration by institutions considering the adopting of biometric markers for authentication.

With conventional (non-biometric) identifiers, when a person is victim to identity theft today, they may ultimately resort to changing their name or identity; as this typically involves non-biometric identifiers such as name, age, and national identifier. This last resort measure is longer applicable to biometric identifiers, since once stolen the person is impacted from that point on and all IT systems that rely upon the stolen biometric marker are also immediately compromised.

Finally, the financial and legal impact that may be felt by an organization that sustains a data breach of biometric data may be considerable and long lasting. The impact may be felt from its customers, the market, regulatory bodies, and competing organizations. While the use of biometric markers is still in its infancy, some of these risks may appear more measured. However, as the technology becomes more widely used and is becomes prevalent, the impacts are likely to grow and become more substantial.

Notwithstanding, where institutions decide to provide a biometric authentication mechanism it seems prudent that at a minimum the user be able to opt-out of using biometric data and be provided with a suitable alternative authentication system that does not involve biometric markers.

Acknowledgment

The authors are employees of the Commonwealth Bank of Australia. Any views or opinions expressed in this article are the author's own and do not necessarily reflect the view of the Commonwealth Bank.

References

[1] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang, "The tangled web of password reuse", *Network and Distributed System Security (NDSS) Symposium*, 2014.

[2] M. Kosmerlj, T. Fladsrud, E. Hjelmas, and E. Snekkenes, "Face recognition issues in a border control environment", in *International Conference on Biometrics (ICB 2006)*, pp. 33–39.

[3] T. Kwon and H. Moon, "Biometric authentication for border control applications", *IEEE Transactions on Knowledge and Data Engineering*, vol. 20, no. 8, Aug 2008, pp. 1091–1096.

[4] S. M. Rahal, H. A. Aboalsamah, and K. N. Muteb, "Multimodal biometric authentication system – MBAS", *Information and Communication Technologies*, vol. 1, 2006, pp.1026–1030.

[5] C. Rathgeb and A. Uhl, "Two-factor authentication or how to potentially counterfeit experimental results in biometric systems", in *International Conference Image Analysis and Recognition (ICIAR)*, 2010, pp. 296–305.

[6] S. Trewin, C. Swart1, L. Koved, J. Martino, K. Singh, and S. Ben-David, "Biometric authentication on a mobile device: a study of user effort, error and task disruption", in *Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC)*, ACM, 2012, pp. 159–168.

[7] L.M. Mayron, "Biometric authentication on mobile devices", *IEEE Security and Privacy*, vol. 13, no. 3, pp. 70–73, June 2015.

[8] C. Senk and F. Dotzler, “Biometric authentication as a service for enterprise identity management deployment: a data protection perspective”, *International Conference on Availability, Reliability and Security*, Aug 2011, pp. 43–50.

[9] Q. Xiao, “A biometric authentication approach for high security ad-hoc networks”, in *Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop*, June 2004, pp. 250–256.

[10] A. Kounoudes,V. Kekatos, and S. Mavromoustakos, “Voice biometric authentication for enhancing Internet service security”, *Information and Communication Technologies*, 2006, vol. 1, pp. 1020–1025.

[11] S. Prabhakar, S. Pankanti, and A.K. Jain, “Biometric recognition: security and privacy concerns”, *IEEE Security and Privacy*, 2003, pp. 33–42.

[12] E. Kindt, “Need for legal analysis of biometric profiling”, in *Profiling the European Citizen, Cross-Disciplinary Perspectives*, M. Hildebrandt and S. Gutwirth. Springer Science, 2008, pp. 139–145.

[13] B. Schneier, “The uses and abuses of biometrics”, *Communications of the ACM*, vol. 42, no. 8, p. 136, Aug 1999.

[14] N. Duta, “A survey of biometric technology based on hand shape”, *Pattern Recognition*, vol. 42, no. 11, pp. 2797–2806, 2009.

[15] L. Ma, Y. Wang, and T. Tan, “Iris recognition based on multichannel Gabor filtering,” in Proceedings of the Fifth Asian Conference on Computer Vision, Melbourne, Australia, 2002, pp. 279–283.

[16] R. Wildes, J. Asmunth, G. Green, S. Hsu, R. Kolczyski, J. Matey, and S. McBride, “A machine-vision system for iris recognition”, *Machine Vision and Applications*, Springer-Verlag, vol. 9, no. 1, pp.1–8, 1996.

[17] J. Daugman, “Demodulation by complex-valued wavelets for stochastic pattern recognition,” *International Journal of Wavelets, Multiresolution and Information Processing*, vol. 1, no. 1, pp. 1–17, 2003.

[18] L. Ma, T. Tan, Y. Wang, and D. Zhang, D., “Local intensity variation analysis for iris recognition”, *Pattern recognition*, vol. 37, no. 6, pp. 1287–1298, 2004.

[19] W. Q. Yan, 2016, “Biometrics for surveillance”, in *Introduction to Intelligent Surveillance*, Springer, pp. 85–92, 2016.

[20] I. Sujit and A. M. Patil, “A review on image-based face recognition techniques”, *International Journal of Engineering Research and Management (IJERM)*, Vol. 2, no. 1, pp. 47–50, 2015.

[21] M. Faundez-Zanuy, “On-line signature recognition based on VQ-DTW”, *Pattern Recognition*, vol. 40, no. 3, pp. 981–992, 2007.

[22] J. Pereira and L. Sher, “How you can help find a missing child on Facebook with new amber alert feature”, *ABC News*, viewed 2 Mar. 2016. [Online]. Available: http://abcnews.go.com/Technology/find-missing-child-facebook-amber-alert-feature/story?id=28173570

[23] The European Child Rescue Alert and Police Network on Missing Children, “AMBER alert Europe partners up with Facebook to save lives of missing children”, AMBER Alert in the news, viewed 2 Mar. 2016. [Online]. Available: http://www.amberalert.eu/amber-alert-europe-partners-up-with-facebook-to-save-lives-of-missing-children/

[24] E. Steel, “How a new police tool for face recognition works”, *The Wall Street Journal*, viewed 2 Mar. 2016. [Online]. Available: http://blogs.wsj.com/digits/2011/07/13/how-a-new-police-tool-for-face-recognition-works/

[25] M. Warman, “Say goodbye to the pin: voice recognition takes over at Barclays Wealth”, *The Telegraph*, viewed 2 Mar. 2016. [Online]. Available: http://www.telegraph.co.uk/technology/news/10044493/Say-goodbye-to-the-pin-voice-recognition-takes-over-at-Barclays-Wealth.html

[26] D. Maltoni, “A tutorial on fingerprint recognition”, in *Advanced Studies in Biometrics*, Springer Berlin Heidelberg, pp. 43–68, 2005.

[27] R. Sharma and M. S. Patterh, “Face recognition using face alignment and PCA techniques: a literature survey”, *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 17, no. 4, Ver. III, p. 17–30, 2015.

[28] T. Mansfield, G. Kelly, D. Chandler, and J. Kane, “Biometric product testing final report”, Centre for Mathematics and Scientific Computing, National Physical Laboratory, Middlesex, UK, 2001.

[29] S. S. Phang, *Investigating and Developing a Model for Iris Changes under Varied Lighting Conditions*, Master thesis, School of Engineering Systems, Faculty of Built Environment and Engineering, Queensland University of Technology, 2007.

[30] C. Zara, “Facebook keeps getting sued over face-recognition software, and privacy groups say we should be paying more attention”, *International Business Times*, viewed 29 Mar. 2016. [Online]. Available: http://www.ibtimes.com/facebook-keeps-getting-sued-over-face-recognition-software-privacy-groups-say-we-2082166

[31] V. Pasupathinathan, J. Pieprzyk, and H. Wang, “Security analysis of Australian and E.U. E-passport implementation”, *Journal of Research and Practice in Information Technology*, Vol. 40, no. 3, August 2008, pp. 187–205.

[32] S. Venugopalan, U. Prasad, K. Harun, K. Neblett, D. Toomey, J. Heyman, and M. Savvides, “Long range iris acquisition system for stationary and mobile subjects”, in *International Joint Conference Biometrics (IJCB)*, IEEE, 2011, pp. 1–8.

ISSN (Print): 2204-0595
ISSN (Online): 2203-173