Biometric Identification: Are We Ethically Ready?

Karen Renaud[1] & Andrew Hoskins[2]
[1]School of Computing Science &
[2]College of Social Sciences
University of Glasgow, Glasgow, Scotland
{karen.renaud;andrew.hoskins}@glasgow.ac.uk

Rossouw von Solms
School of ICT
Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
Rossouw.VonSolms@nmmu.ac.za

Abstract—***"Give us your fingerprint, your Iris print, your photograph. Trust us; we want to make your life easier!"*** **This is the implicit message behind many corporations' move towards avid collection and use of biometrics, and they expect us to accept their assurances at face value. Despite their attempts to sell this as a wholly philanthropic move, the reality is that it is often done primarily to ease their own processes or to increase profit. They offer no guarantees, allow no examination of their processes, and treat detractors with derision or sanction. The current biometric drive runs counter to emergent wisdom about the futility of a reductionist approach to humanity. Ameisen *et al.* (2007) point out that the field of integrative biology is moving towards a more holistic approach, while biometrics appear to be moving in the opposite direction, reducing humans to sets of data with cartographic locators: a naïve over-simplification of the uniqueness that characterizes humanity. They argue that biometrics treat the body as an object to be measured, but in fact the body is a subject, the instantiation of the individual's self, subject to vulnerability and mortality. Treating it merely as a measured and recorded object denies the body's essential right to dignity. Here we explore various concerning aspects of the global move towards widespread biometric use.**

Keywords: biometrics; security; ethics.

I. INTRODUCTION

The 'connective turn' [22][23] has ushered in a living archive of networked consumers: a new mass public requiring regular and frequent access to machines, to services, and to others. This 'turn' is an emergent set of tensions and transitions from a 'scarcity' to a 'post-scarcity' culture ushered in by the abundance, pervasiveness and accessibility of communication networks, nodes, and digital media content.

In this environment, the basics of personal identity, privacy and individual and social memory, become increasingly entangled with networked literacies: our capacity to navigate, contribute, organize, order, classify, search, and retrieve digital content. These digital technologies and modes of communication have significantly infiltrated our personal and public selves and relationships, to an extent that our lives seem unthinkable without media. Mark Deuze, for instance proposes that media studies as a discipline '*should take as its point of departure a view of life not lived with media, but in media*' ([13]: 49ff).

This 'media life' perspective manifests itself across a whole swathe of personal, social and cultural phenomena. It is particularly indicative of a period in which the biological, social and technological domains, which have historically often been seen and studied as quite separate fields, are being explored more dynamically, holistically and as part of the same 'ecology'. The growth of Science and Technology Studies (STS) and Human Computer Interaction (HCI) have contributed to this paradigm-shift.

In this paper we explore the development of biometrics as a technological means successfully to identify and/or verify individuals. We explore some ethical aspects as prerequisites to guarantee widespread user acceptance thereof. Biometrics are essentially technologies that measure and analyze characteristics of the human body to enable authentication of the user. As such, they are inextricably a security-of-the-self. These include: facial recognition, fingerprints, eye retinas and Irises, and voice patterns. Our concern here is how biometrics 'technologize' a memory-of-the-self, and particularly through their convergence with the domain of corporate security.

By the 'technologization' of memory, we build on emergent work in the field of Memory Studies which has begun to grasp some of the dynamics of what might be called the 'mediatization' of memory and how the making of memory is increasingly embedded in and distributed through our 'sociotechnical practices' [9][40][19]. Memory has long been characterized through the separation of or tension between the internal (mind and body) and the external (representations, media etc.) domains [14]. Yet biometrics undermine the very basis of this distinction through taking the relatively contained uniqueness of the self and distributing it through an unpredictable media ecology. In these circumstances, biological matter acquires a qualitatively different status; it becomes 'informational' ([8]: p.7). That is, it becomes subject to connectivity, to the logics and (in)securities of the network. Once biological matter and the formation and reformation of memory from this matter are made informational, then the function, ownership, uses and abuses of memory are more-or-less lost to the self. Instead, it is the keepers of the network that determine how one's past is stored and strewn across the new media ecology.

Meanwhile, the technologization of security is tied to the inexorable rise of computing and networking. In the early days of computing, networks were relatively limited in their numbers of users, and the ancient and well-understood technique of the password served the security of these systems perfectly well. Today, the humble password is under severe strain, made fallible through its exponential use, both for users who have to devise passwords, and for systems that have to recognize each individual in the digital crowd with a

978-1-4799-7755-0/15/$31.00 ©2015 IEEE

reasonable level of certainty that will stand up to legal scrutiny in some cases.

Requiring users periodically to change passwords, in an attempt to improve security, to contain the sharing and proliferating use of the same password across systems, is a flawed measure. The greater the frequency of the forced change, the less likely it is that it will be retained in human memory, and the greater the likelihood of it being written down to safeguard against loss. Moreover, the computer screen is both the most convenient and the most public repository for the password (written on a post-it note).

Passwords are fundamentally shareable, passed around, loaned out, lent to another when the authorized user is unavailable or wants to delegate [12]. In many ways then, authenticating based on what someone knows does not prove identity: it only confirms shared knowledge, knowledge that can easily be transferred to another, either deliberately or inadvertently. Whereas the password performed well when used by small populations of technical users, when it went global it became obvious that the mechanism did not scale satisfactorily.

To address the challenges of memorability and the insecurity of sharing, many service providers are turning to biometrics. What is not easily memorable needs to be externalized: and after the connective turn some argue that modern memory is less about remembering and more about knowing where to look. Biometrics returns memory to the self. They displace the vagaries and uncertainties of the external and the collective worlds.

This investment in the memory of the security of the self also requires a certain divesting of the self. The password shared, copied and lost is ultimately replaceable. However, biometrics work through the guarantor of relative uniqueness, a uniqueness that, once lost, is not retrievable.

Biometrics are widely used by government agencies that have traditionally held a certain degree of public trust in their use of personal data, or at least in situations that did not include an element of choice. For instance, many countries capture biometrics before issuing passports: those who are uncomfortable with this are not accommodated; they simply cannot travel abroad unless they acquiesce. Unfortunately the competence of such agencies in recent years has been suspect [4]. A series of national scandals in the accumulation of database records, lost [11], hacked or misplaced, or 'accidentally' made public, has dissipated public trust in those charged with the protection and preservation of our most personal data.

Corporate managers of private information have been shown to be more even more susceptible to such scandals [5]. Thus, the spread of the use of biometrics into this particularly shaky sphere of personal security, through the unevenness of its regulation and accountability, seems a risky move for the biometric giver, but with very little cost to the biometric recorder. As such, the power relationship is skewed in favor of the corporation, at the expense of the employee or customer.

II. Defining Biometrics

Biometrics appear to address the memorability and sharing problems of passwords in one fell swoop. There are two distinct kinds of biometric:

Physiological

Often referred to as "*what you are*". Examples are fingerprints, Iris scans and faces. More esoteric biometrics include ear prints, gait analysis and even eyeball reflex patterns. Most biometrics require additional hardware to be able to "read" the biometric and to compare it to the previously recorded pattern.

Behavioural

Referred to as "*what you do*". This kind of biometric collects information as you use a device, perhaps while you type or speak into the microphone. The biometric then stores a template that represents your common patterns. When you use the device again the biometric system compares your current usage with the master pattern and generates a percentage level that indicates the level of matching between the two.

Passwords and PINs can implement a binary decision: the secrets either match or they don't. If they do, the person gains access, otherwise access is denied. Authenticating with biometrics constitutes a less clear-cut process. Biometrics commonly deliver a confidence level, a percentage that indicates how well the newly collected and stored templates match. Many factors can interfere with this process: changes in the human due to injury or age, faults within the equipment or simply the result of a poor "reading". The system bases its decision according to a risk threshold. For example, if the threshold is set to 90%, and the matching delivers a confidence of 89% the person will be rejected. Any confidence level above 90% will result in the person being authenticated. Two types of errors result from the use of biometrics confidence levels:

1. *False Reject*, when a genuine user is rejected;
2. *False Accept*, when an imposter is erroneously authenticated.

Systems are usually tailored to minimize these errors and to reflect the risk associated with the service being protected. So, for example, a biometric that grants access to a bank account might require a 99% matching confidence whereas a biometric that allows you to pay for a meal in an employee canteen could be set much lower.

Jain *et al.* [24] propose a set of requirements that help to identify a viable biometric:

- *Universality*, which means the majority of people should possess the biometric;
- *Distinctiveness*, which means that the particular characteristic is sufficiently different between humans to support identity verification;
- *Permanence*, the characteristic does not change significantly over time;
- *Collectability*, which means we can quantify the measurement which facilitates automated comparison;

- *Performance*, the fact that the biometric can be matched accurately, speedily, with reasonable resources.

The first aspect is not as easy to satisfy as it seems at first glance. About 2% of the US population does not have a fingerprint that can be read [31]. Other biometrics, such as facial biometrics, are more universal, but deliver much higher error rates, since distinctiveness is far poorer than it is for fingerprints. Fingerprints also fail the permanence characteristic since females' fingerprints become less prominent as they age [37], which makes them difficult to capture with biometric readers. Some kinds of chemotherapy appear to remove fingerprints altogether [21]. Sometimes biometrics are combined to deal with potential problems with one particular biometric. So, for example, both fingerprint and face could be used in tandem to deliver a more reliable decision making process.

An issue that Jain *et al.* [24] do not address is the invasiveness of the biometric reader. Invasiveness is a key aspect in whether people will accept the mechanism. Some biometrics, such as retina recognition, require the person to place their eye directly into a reader. On the other hand, some biometrics can be collected without the person's knowledge, which means a potential attacker could collect and use the recorded biometric for nefarious purposes, without the owner's knowledge.

This brings us to a related characteristic, the ease with which a biometric can be copied. It is very difficult, but not impossible [18], to copy an Iris, but trivial to copy a voice or facial biometric. A copy can sometimes be used to fool the system into a false-accept decision. Usually, the more invasive a biometric reader, the harder the biometric is to copy. The other problem is related to the storage of the collected biometric template. Because of the indelible link to the true self, biometric templates have to be stored securely and protected far more assiduously than one does a password.

The final characteristic is cost. The cheapest biometric readers are often the ones most easily fooled. The optical fingerprint reader, for example, is cheap and easily fooled by false fingers. The capacitance fingerprint readers, which test for liveness, are not as easily fooled but are also more expensive. Organizations will inevitably play off risk levels against the cost of readers which means that much-vaunted benefits of biometric usage often are not realized, so the customer's privacy and rights have potentially been violated to no avail. Yet since the true "cost" is borne by the customer, the unreliability and untrustworthiness of the reader does not impact on the organization or hurt their profit margin.

One of the most controversial biometrics is DNA. It is easily collected, without the consent or knowledge of the human source. The FBI used saliva from stamps to identify a World Trade Centre bomber [30], which was probably never anticipated by the person sending the letter. Researchers, for some time now, have been ringing alarm bells. Nelkin and Andrews cite Foucault [17] who warned that knowledge could be used to gain power. He hypothesized that tests would deliver the means to compare, differentiate and exclude. Nazi Germany's persecution of people based on their heritage is a stark example of this. Magnet [27] explains how this kind of undesirable profiling can be supported by the use of biometrics.

Nelkin and Andrews [30] report that the US military have decided to collect DNA samples from all their soldiers. They appear to have perfectly sound reasons for the collection of DNA samples: to identify soldiers killed in battle, to solve crimes. Yet some marines declined to comply. Those US marines who refused to have their DNA collected cited previous examples where the US government had failed to act in their interests, and coldly sacrificed soldiers for their own aims. Nelkin and Andrews mention Agent Orange usage in the 1970s and the fact that soldiers were told to watch nuclear bombs going off when the tests were carried out. One can hardly blame the soldiers for their skepticism. One could consider these lapses by the US government an aberration - we want to feel we can trust our government [20]. On the other hand no one expects corporations to be trustworthy: we know that they act in their own interests. A prime example is that of Google, whose CEO, after the UK government attempted to shame the company for their very successful tax avoidance schemes, triumphantly expressed pride in having pulled off the feat [39]. Expecting corporations to be moral is clearly naïve.

The following section provides an example of the use of biometrics by a business in Glasgow

III. BIOMETRIC USAGE EXAMPLE

In October 2011 [6] a Glasgow nightclub announced that it would be using fingerprints to verify the age and identity of its customers. They claimed that this was being done in order to "tackle the city's alcohol problems." Such a sweeping claim demands further scrutiny. Closer examination raises the following questions and conundrums:

- Are they suggesting that their current, flawed, access control mechanisms, for the three venues in question, are significantly contributing to Glasgow's alcohol problems? Surely their contribution is fairly minor, given the size of Glasgow and the number of places people can buy alcohol.
- Are they suggesting that they currently have significant problems inadvertently supplying alcohol to underage children, such that it warrants expenditure on such a system? Firstly this is debatable since UK legislation is very strict [9]. Secondly, they can, without incurring any cost at all, require everyone who looks under 25 to prove their age using an official identity document. The BBC [3] claims that 25% of underage drinkers get the alcohol from an older adult. The same news article suggests that off-licences are selling alcohol to underage drinkers, and this is confirmed by another news report [16]. No mention is made of nightclubs in either report so their contribution to the underage drinking problem is probably minor.
- Indeed, many young people already carry a convenient form of identity with them: their driver's license. The Scottish Government [36] reports that 60% of males in the 20-24 age range possess driver's licenses, with just under 50% of women driving. Is the fingerprint reader really better than this widely-accepted mechanism, which also bears a biometric: the person's face? A number of clubbers

will also possess passports. A valid form of identification is mandatory to register for the touted fingerprint scheme. One wonders why this cannot be used to prove age at every visit.

- The clubs do not appear to offer their customers the opportunity to opt out. Indeed, a web log[1] confirms that at least some customers are not being offered any choice or that the fingerprints are being recorded while they are inebriated. Moreover, staff at the club the blogger is complaining about did not know where the data was being held, or who had access to it.
- The scanner being used appears to be the Scannet. The manufacturer's website[2] provides guidance from the UK information commissioner, acknowledging the very personal nature of the data being collected. One can therefore understand the club's attempt to market this endeavor with the claim that they are solving a huge social problem in Glasgow. They are clearly hoping to offset any criticism that might result should customers realize that their personal data is being held by the nightclub for an undisclosed period of time. The FAQ page[3] revealed that a facial image was also being collected by the system, supporting multi-modal biometric use, even more invasive than a single mode biometric.
- Mackenzie [25] says, while proclaiming the excellence of the scheme: "*Citti said it provides huge scope when it comes to marketing*". Here the nub of the matter is revealed. The real purpose behind the scheme is the opportunity it affords to perform market segmentation and to track clubbers' attendance and behaviour in the clubs. This is also alluded to on the manufacturer's website.

Hence the scanning of clubbers' fingerprints has less to do with tackling the city's alcohol problems than with (1) making things more convenient for bouncers, and (2) making even more money from clubbers by being able to target them, and their wallets, far more intelligently. The real motivator is profit, and the maximization thereof, while the rights of customers are being sacrificed. However hard we look at this example, the only minor advantage to the clubber is that they no longer have to carry identity cards. This seems a very small benefit in return for giving a club access to such very personal details as fingerprints and behaviour logging. Moreover, surveys suggest that people will accept the use of biometrics for law enforcement and immigration purposes, but they less supportive of the use of biometrics for access control or attendance monitoring [15]. It is puzzling that people will willingly give their fingerprints to this nightclub. One can only surmise that the touted convenience is so enticing that they do not give sufficient thought to what they are giving away.

IV. Vulnerability of Biometric Collection Systems

Figure 1 demonstrates a simplified architecture for collecting and using biometrics. Whereas the purveyors of these systems claim impressive levels of reliability, the reality is somewhat less impressive. Each component of the diagram is vulnerable to attack but even if no one attempts to compromise the integrity of the system it can still deliver the incorrect decision. Enrolment is the key to the success of later use. If the initial feature vector is suboptimal or poorly recorded the person might well experience difficulties being authorized at later access attempts.

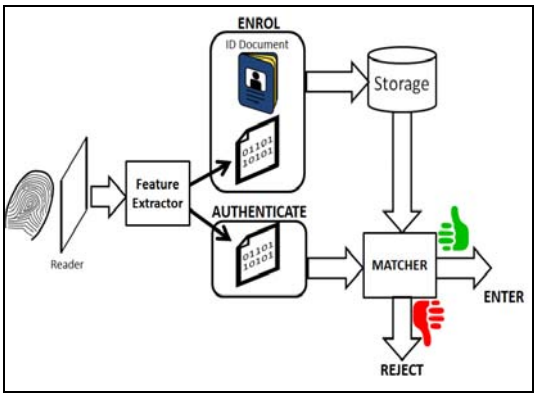

Figure 1. Biometric Collection and Verification

Sometimes the reader cannot read the person's fingerprint correctly when they return at a later date, due to an injury or some other reason outwith their control. The legitimate person will be denied entry to the club: an undesirable event given their potential for spending money. The system also has a number of important operational needs. The sensor that reads the fingerprint relies on an uninterrupted power supply, the right levels of humidity, moderate temperature and a clean surface. The manufacturers of the scanner used in the nightclubs in Glasgow said this on their FAQ website[3]: "*The scanner could be dirty i.e. from moisturiser THE ONLY WAY TO CLEAN your scanner is by placing sellotape across the screen and lifting - DO NOT RUB WITH A CLOTH OR LICK*".

If use of the reader is not carefully monitored it is likely that people could use fake fingerprints to "spoof" the reader. Thus a supervisor needs to monitor the use thereof continuously. If the database is compromised, the integrity of the stored records becomes suspect, which renders matching decisions untrustworthy. The constituent parts need to communicate with each other and in systems where the components reside on different hardware the communication can also be subverted. In the example given above, all the components appear to be situated within a single hardware box, making it easier to resist such attacks. Unfortunately, Scannet publish their default password on their FAQ website. Given the fact that very few people change default passwords, as evidenced by the phone hacking scandal of 2011 [28], this means that the data is potentially unprotected and unsecured. If the security of the records is suspect, this renders the entire mechanism less trustworthy. Even a superficial scrutiny of this scheme reveals security and operational flaws, convincing the authors of this paper to give these nightclubs a miss.

[1] http://forums.pepipoo.com/lofiversion/index.php/t66824.html

[2] http://nightclub.co.uk/downloads/CustomerNotice-A3_d.pdf

[3] This advice has now been removed

V. More Biometric Usage Examples

Figure 2 provides some examples of the use of biometrics by big business across the world. The concern, with all of these uses, is whether the customer or employee retains the right to opt out. It was not possible to confirm or deny this from the news reports.

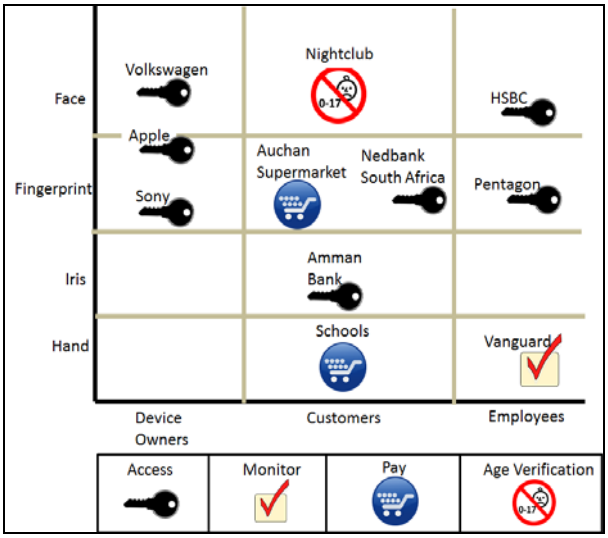

Figure 2. Examples of the use of Biometrics by Corporations (Appendix A)

The problem we seek to highlight is that human rights very seldom enter the equation when biometrics are deployed by big business. People are simply expected to comply with the demands of organizations that decide to deploy biometrics for a variety of purposes, usually because the biometric makes things easier for them, not because of customer or employee demand. This is demonstrated very well by the practices of Nedbank in 2011 (**Figure 4**). Their implementation required anyone visiting their branches to present a fingerprint to gain entry[4]. There was an outcry from various citizens [5] especially since the company says that they will share the data, but do not specify who the recipients of such shared data will be, or the pretexts under which this will occur. The blog in **Figure 3** suggests that customers were not even given the opportunity to opt out of the scheme [6]. Nedbank has reportedly now abandoned this scheme[7].

One wonders which third parties they provide their databases to (as stated on their poster in **Figure 4** - bottom right). Finally, many 21st century companies are global, which raises some important questions with respect to their use of biometrics. Where is the biometric data actually stored? It could be stored in the cloud, which is probably located in another country. The UK has very strict laws about storage and protection of personal data, and much of the European Union mirrors these. Other countries are far more *laissez faire* with personal data. Once a UK customer's biometric data leaves the UK's jurisdiction, and protective laws, how well will it be protected? How are those who wish to use this data for nefarious purposes to be prevented from doing so? If the UK government cannot even make multi-national companies pay fair taxes [39] how will they protect individual citizens' personal biometric data when it is held in another country.

Figure 3. Blog ("*Just went to Nedbank in Pinetown and was surprised to see that prior to entry I had my photo and fingerprint taken. The branch manager couldn't tell where my data is stored or for how long it is stored. Is this legal?*" Posted 4 April 2012)

VI. Ethics Considerations

Biometrics might well not be the panacea they're often touted as. They are indelibly bound up with our person, and thus inherently part of whom we are. For everyone promoting biometrics as the silver bullet to solve all identification problems[8] there is someone else expressing grave concerns about their increasingly widespread use[9]. Sylvia Venier [41] posed the following challenging questions regarding biometrics and multiculturalism:

- Whether ethnicity can be derived from biometric data
- Whether different ethnic groups find it more or less problematic to participate in biometric identification
- Whether there might be a risk of discrimination against minorities
- Whether any risk exists that groups of people can be categorised through profiling.

Obviously these are very challenging questions from an ethics point of view and, according to Venier [41], no research results have provided any clear motivations to ignore any of these highly contentious ethical issues.

Except for the general ethical issues identified by Venier above, two very specific and sensitive ethical aspects still remain problematic; that of social exclusion and privacy.

From prior research it is clear that there are always going to be some individuals or groups of people who cannot reliably enroll or verify some or all of their biometrics [43]. He further points out that false negatives could have disastrous effects on

[4] http://www.moneyweb.co.za/moneyweb-financial/nedbank-pilots-branch-biometric-access-control
[5] http://medialternatives.com/2012/01/04/nedbanks-biometric-bungle-exposes-personal-info-bill-shortcomings/
[6] http://www.thehubsa.co.za/forum/topic/114903-nedbank-collecting-fingerprints/
[7] http://medialternatives.com/2013/01/16/nedbank-abandons-its-biometric-fingerprinting-devices/
[8] http://www.hitachi.com/rd/yrl/people/info_security/03.html
[9] http://www.bigbrotherwatch.org.uk/home/2012/08/are-you-ready-to-provide-your-fingerprint-on-demand.html#.UKCK8YZk1GM

Figure 4.. Nedbank's Customers gain access to branches using their Fingerprints
(bottom para: "*Nedbank will only process and act upon the personal information supplied for purposes of the appropriate internal and external reporting to prevent crime and to pursue its own legitimate interests and those of third parties to whom the personal information is supplied*")

people's lives, but, "*not being able to drive away in one's car, or boot a computer could be bad enough, but consider the stress that would be suffered if your facial biometrics was rejected at passport control*." Also, some groups of people are more likely to be disadvantaged by the use of biometrics, like; people with physical disabilities, those with mental illness, the elderly, people of certain races, people of certain religions and the homeless [43].

There are many who consider the collection and use of biometrics a privacy violation that ought not to be imposed on people who are uncomfortable with their use. Solove [38] delineates privacy as follows:

> "*privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations*" (p. 1)

He also argues that privacy is the cornerstone of freedom, democracy and psychological well being. Back in 1967 Westin [42] expressed concerns about the impact of surveillance on privacy. Today people are even more concerned, since organizations often put their own convenience ahead of the privacy rights of their customers or employees. A prime example is that British schools are collecting biometrics of children without parents' consent [35]. Yet another example is that the UK police will be compiling a database of photos of people who have not committed any crime [32].

Specific concerns relate to how biometrics will be stored, who will have access to them, what purpose(s) they will be used for, and how reliable biometric authentication is. To address concerns about the biometric being compromised if a biometric database is accessed by an unauthorized person, the biometric is not stored as an image: it is stored in digital format which cannot easily be used to reconstruct the original biometric. However, new attacks emerge yearly, which show that it is possible for biometric templates, previously considered invincible, to be compromised [18].

The concerns with respect to unauthorized access are well founded. Biometrics are classified as personal data, and in the UK this means that the organization holding the data has to comply with the Data Protection Act of 1998. However, a recent survey by the BSI[10] found that one in five businesses admitted breaching this act. The UK information commissioner announced in August 2012 that data breaches had increased tenfold in the last five years [7]. This proves that organizations probably cannot be trusted to look after our personal data. When this data is a biometric its loss is far more serious than the loss of a mere password.

However, the emergent ethics, social and political ramifications of the growing use of biometrics are also entwined with the prospects of a memory that is not prone to

[10] http://shop.bsigroup.com/en/Browse-By-Subject/Data-Protection--Freedom-of-Information/

natural and healthy forgetting. For instance, a 'right to be forgotten' is now included in Article 17 of the European Commission proposal for a General Data Protection Regulation [25]. In diffusing control over memory-of-the-self, what threats do the corporate spread of biometrics pose to attempts to establish and protect the right to be forgotten?

Nelkin and Andrews [30] quote a US marine who refused to give a DNA sample to the US military. He said: "*Your body is one of the few things you have control over*". Yet when various measures of our bodies are encoded and stored by untrusted entities, with no recourse offered should they divulge or fail to protect it, do we still have control over our bodies? Are customers sacrificing this without thought, to their own detriment? Google trends (**Figure 5**) provides a snapshot indication of concern about biometrics over time and it seems that people are becoming sufficiently accustomed to their use that they no longer feel as great a need to seek out more information. Corporations are slowly habituating us to their use of biometrics so that we accede to their demands for our most personal information. Unfortunately, in becoming accustomed to anything, we run the risk of not seeing its dangers, and biometrics are no exception.

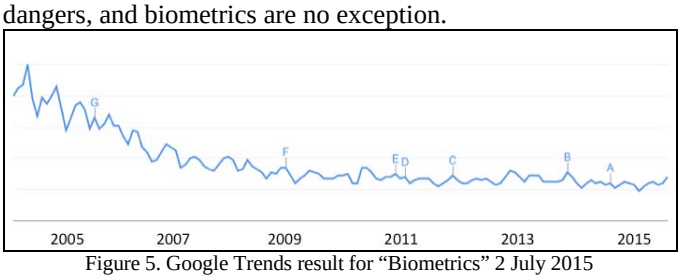

Figure 5. Google Trends result for "Biometrics" 2 July 2015

Mayhew [29] reports that the Indian government will be collecting biometric data from some of their most vulnerable citizens: orphaned and fostered children. The cited reason is: "*These measures are adapted as a means to prevent another Rohtak shelter incident from happening, where children were allegedly sexually abused and tortured*". Raza [33] relates how the staff in these homes subjected the children to horrific abuse. It is not clear how collecting the children's biometrics is meant to prevent such abuse; neither report explains this. It is particularly concerning that the most vulnerable members of society have their biometrics collected without anyone acting to ensure that it is indeed warranted and justified, and it is unlikely that this will prevent abuse as they hope it will. Along with this, the issue of social exclusion is a definite ethics issue. It boils down to sacrificing some people in the interests of others [43]. From the above, it is clear that biometrics, from a technical point of view, will not be viable unless these ethical concerns have been satisfactorily addressed.

VII. Conclusion

Historically, organizations have had patchy records in guarding the safety of their employees. For example, workers were sometimes expected to carry out dangerous jobs without the right equipment or protection. The Forth Bridge visitor centre in Scotland claims that 63 people died building the bridge. Yet no workers died during the building of the entire Olympic village that opened in 2012. This is no doubt at least partly due to the health and safety regulations that are strictly enforced within the UK, preventing employers from putting their workers at risk and mandating safety practices.

Unfortunately, we cannot expect corporations to behave morally because it is the right thing to do: their focus is to maximize return on investment and some often act as if the end justifies whatever means they can employ to achieve this. The worldwide recession we are currently experiencing has been attributed directly to the rash behavior of bankers **Error! Reference source not found.**. That said, there are two central ways for people to be protected from the exploitation of big business. The first is for legislation to be passed that prevents companies from specific exploitative practices. Indeed Rose and Spiegel [34] report that countries with looser credit regulations appeared to have suffered the worst crises, which seems to confirm that bad behaviour by banks, unchecked by legislation, played a role in causing this recession. Companies are often ingenious in marketing biometric use in ways that make it seem legitimate and perfectly reasonable. Lawgivers are thus not sufficiently concerned to enact laws. The only viable (and second) option, therefore, is for people to act to protect themselves. Declining to have our biometrics collected is the only secure means, i.e. our watchword should be: "*Caveat Humana*": retain your individuality and your right to your own body

References

[1] Acharya, V. V., & Richardson, M. (2009). Causes of the financial crisis. Critical Review 21(2-3), pp. 195-210.

[2] J-C. Ameisen, S. Beloucif, P. Cossart, M. Delmas-Mart. et al., (undated "Biometrics, identifying data and human rights," Opinion No 98. National Consultative Ethics Committee for Health and Life Science, 2007. http://www.comitedebioetica.es/documentacion/docs/biometric_identifying_data_and_human_rights.pdf, Accessed 2 July 2015.

[3] BBC. (2004) Blitz targets under-age drinking. 2004. http://news.bbc.co.uk/1/hi/scotland/3905973.stm

[4] BBC. (2008) Government loses one PC a week. 21 November 2008. http://news.bbc.co.uk/1/hi/uk_politics/7740593.stm

[5] BBC. (2008) Company loses data on criminals. 21 August 2008. http://news.bbc.co.uk/1/hi/uk/7575766.stm

[6] BBC. (October, 2011) Glasgow Nightclubs start using fingerprint data, 7 October 2011. http://www.bbc.co.uk/news/uk-scotland-glasgow-west-15215019

[7] BBC. (2012) Data breaches 10 times worse, say ICO figures. 30 August 2012. http://www.bbc.co.uk/news/technology-19424197

[8] L. Blackman. (2012) Immaterial Bodies: Affect, Embodiment, Mediation. London, UK: Sage.

[9] G. C. Bowker. (2005) Memory practices in the sciences. Cambridge, MA: Mit Press.

[10] Clitheroe Advertiser and Times. (2011) Clitheroe pub loses licence after underage sales. 20 December 2011. http://www.clitheroeadvertiser.co.uk/news/local-news/clitheroe-pub-loses-licence-after-underage-sales-1-4076204

[11] Computer Weekly. (2007) UK Government loses data on 25 million Britons. 20 November. http://www.computerweekly.com/news/2240084015/UK-government-loses-data-on-25-million-Britons

[12] F.J.Corbató. (2007) On building systems that will fail. In ACM Turing award lectures. ACM, New York, NY, USA. 2007

DOI=10.1145/1283920.1283947 http://dx.doi.org/10.1145/1283920.1283947

[13] M. Deuze. (2010) Media Work. Cambridge: Polity Press.

[14] M. Donald. (2002) A Mind So Rare: The Evolution of Human Consciousness. London: W. W. Norton.

[15] S. J. Elliott, A. S. Massie, and M. J. Sutton. (2007) The perception of biometric technology: A survey. Automatic Identification Advanced Technologies, IEEE Workshop on.

[16] K. Foster. (2012) Off-licences worsen teenage drinking, report warns. News.scotsman.com. http://www.scotsman.com/news/health/off-licences-worsen-teenage-drinking-report-warns-1-2694321

[17] M. Foucault. (1979) Discipline and Punish. New York: Vintage Books.

[18] J. Galbally, A. Ross, M. Gomez-Barrero, J. Fierrez, and J. Ortega-Garcia. (2012) From the Iriscode to the Iris: A New Vulnerability of Iris Recognition Systems White paper for Black Hat USA. http://www.blackhat.com/usa/bh-us-12-briefings.html

[19] R. Grusin. (2012) Premediation: Affect and Mediality After 9/11. Basingstoke: Palgrave Macmillan.

[20] R. Hardin. (1999) Do we want trust in government? in Democracy and Trust. Ed: M E Warren. Cambridge: Cambridge University Press.

[21] K. Harmon. (2009) Can you lose your fingerprints? Scientific American. http://www.scientificamerican.com/article.cfm?id=lose-your-fingerprints

[22] A. Hoskins. (2011) 7/7 and Connective Memory: Interactional trajectories of remembering in post-scarcity culture. Memory Studies. 4(3), pp. 269-280, 2011.

[23] A. Hoskins, (2012) Media and Memory. Cambridge MA: MIT Press.

[24] A. K. Jain, A. Ross, and S. Prabhakar. (2004) An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), pp. 4–20.

[25] C. Kuner. (2012) The European Commission's proposed data protection regulation: A copernican revolution in European data protection law. Bloomberg BNA Privacy and Security Law Report, February 6, 1-15.

[26] G. Mackenzie. (2011) City clubbers give scanner thumbs up. Scottish Licenced Trade News, 27 October 2011. http://sltn.co.uk/2011/10/27/city-clubbers-give-scanner-thumbs-up/.

[27] S. A. Magnet. (2012) When Biometrics Fail: Gender, Race and the Technology of Identity. USA: Duke University Press.

[28] R. Manne, R. (2011) Bad news: Murdoch's Australian and the shaping of the nation. Quarterly essay. 43(1).

[29] S. Mayhew. (2012) Orphan children in Haryana, India subject to biometric data gathering. Biometric Update.com. http://www.biometricupdate.com/201207/orphan-children-in-haryana-india-subject-to-biometric-data-gathering/

[30] D. Nelkin, and L Andrews. (2003) Surveillance Creep in the Genetic Age. In D Lyon (Ed.) Surveillance as Social Sorting: Privacy, Risk and Social Discrimination. London: Psychology Press.

[31] NIST. (2002) Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability. NIST, Tech. Rep, 2002. http://biometrics.nist.gov/cs_links/pact/NISTAPP_Nov02.pdf

[32] P. Peachey. (2012) Police Launch Mugshots Database to Catch Criminals Moving Around the Country. http://www.independent.co.uk/news/uk/crime/police-launch-mugshots-database-to-catch-criminals-who-move-around-the-country-8304983.html

[33] D. Raza, D. (2012) A crying shame: sexual abuse in children shelters. Firstpost. http://www.firstpost.com/india/a-crying-shame-sexual-abuse-in-children-shelters-348852.html

[34] A. K. Rose and M. M. Spiegel. (2011) Cross-country causes and consequences of the crisis: An update. European Economic Review, 55(3), pp. 309-324, 2011.

[35] K. Sellgren. (2010) Warning over pupil fingerprinting. BBC News. http://news.bbc.co.uk/1/hi/education/8593727.stm

[36] Scottish Government. (2011) High Level Summary of Statistics Trend. Last update: Friday, September 23, 2011. http://www.scotland.gov.uk/Topics/Statistics/Browse/Transport-Travel/TrendDrivingLicense

[37] N. C. Sickler, and S. J. Elliott, (2005, October). An evaluation of fingerprint image quality across an elderly population vis-a-vis an 18-25 year old population. In Security Technology, 2005. CCST'05. 39th Annual 2005 International Carnahan Conference on (pp. 68-73), 2005.

[38] D. Solove. (2008) Understanding Privacy. USA: Harvard University Press.

[39] Daily Telegraph. (2012) Google's tax avoidance is called 'capitalism', says chairman Eric Schmidt. http://www.telegraph.co.uk/technology/google/9739039/Googles-tax-avoidance-is-called-capitalism-says-chairman-Eric-Schmidt.html

[40] N. Van House and E. F. Churchill. (2008) Technologies of memory: Key issues and critical perspectives. Memory Studies. 1(3), pp. 295-310.

[41] S. Venier, (2009) Ethical aspects of Biometric Identification Technologies in a Multicultural Society. unpublished, 2009. http://www.cssc.eu/public/EACME%20ANNUAL%20MEETING%20ppt.pdf

[42] A. Westin. (1967) Privacy and Freedom. New York: Atheneum.

[43] J. Wickins. (2007) The ethics of biometrics: The risk of social exclusion from the widespread use of electronic identification. Science and Engineering Ethics, 13(1), pp. 45-54.

VIII. APPENDIX A

HSBC: http://www.ekoo.co.uk/news/195--hsbc-paves-the-way-with-installation-of-biometrics.html
Vanguard Group: http://www.clarkhoward.com/news/clark-howard/consumer-issues-id-theft/vanguard-experimenting-new-voice-recognition-biome/nCG4Q/
Dubai Airport: http://www.aviationpros.com/news/10816001/aoptix-offers-id-verification-system-at-dubai-international-airport
Auchan Supermarkets: http://www.planetbiometrics.com/article-details/i/1315/
Apple: http://www.securitymanagement.com/news/apple-files-biometrics-patent-iphone-and-mac-computers-005426
Volkswagen: http://www.volkswagenag.com/content/vwcorp/content/en/innovation/communication_and_networking/Biometric.html
Nightclubs: http://www.nightclub.co.uk/news/index.php?m=10&y=11&entry=entry111007-144550#axzz2Bwbf6qN5
Sony: http://www.sony.co.uk/hub/discover-vaio/5
Cairo Amman Bank: http://www.biometricupdate.com/201210/cairo-amman-bank-uses-biometrics-to-register-100000-customers/
UK Border Agency: http://www.ukba.homeoffice.gov.uk/customs-travel/Enteringtheuk/usingiris/
Pentagon: http://www.smartplanet.com/blog/smart-takes/pentagon-using-biometrics-for-smarter-warfare-facilities-business-processes/10058
Univ California: http://voices.yahoo.com/the-biometric-identification-universities-59931.html
Standard Life: http://www.finextra.com/news/announcement.aspx?pressreleaseid=7962