The Relationship between Biometric Technology and Privacy: A Systematic Review

Zibusiso Dewa
School of Computer Science and Informatics
De Montfort University
Leicester, UK
zibusisodewa@gmail.com

***Abstract*—As the demand for biometric technology grows its very implementation appears poised for broader use and increased concerns with regard to privacy have been raised. Biometric recognition is promoted in a variety of private and government domains, helping to identify individuals or criminals, provide access control systems to enable efficient access to services, helping keep patient data safe amongst other functions. However, new advances in biometrics have brought forth widespread debate amongst researchers with concerns surrounding the effectiveness and management of biometric systems. Further questions arise about their appropriateness and societal impacts of use. This review begins by providing an overview of past and present biometric technological uses and the serious problems they pose to privacy. It then factors that play a part in the implementation of privacy in biometrics. The cultural differences that affect legislative approaches are explored, through comparing the approaches adopted by the European Union and the United States. Furthermore, possible methods of remediating the concerns raised by the implementation of biometrics are discussed. It is concluded that Governments and organisations must be transparent and cooperate with legislators, this combined effort may eliminate many of the perceived risks in the technology and help elucidate clearer methods for governing biometrics, to ensure that future developments hold privacy at a high regard.**

Keywords—Biometric technology; privacy; legislation; evolving practices; invasiveness; conflicting interests; European Union

I. INTRODUCTION

As the digital technology realm continues to grow at an uncontrollable rate, showing no sign of slowing down, each widespread development is felt globally and significantly impacts our digital environment [1]. Through widening the scale of digital security and forming new privacy challenges they require us to evolve in our methods of identifying potential risks and managing them [1].

A report by the Organisation for Economic Co-operation and Development (OECD) outlines that the management of risks in terms of security and privacy are essential if countries and organisations are to access the range of social and economic benefits of this digital economy [2]. One of the major factors that affect the rate at which technology is implemented, adopted and accepted by society is Trust [2]. It is no surprise that high levels of trust amongst the public tend to enable a harmonious widespread acceptance and implementation of the technologies and the organisations usage of the technology. Regulators, policy developers, privacy commissioners and privacy advocates are important as they can encourage public debate, establish and enforce legislation and safe data practices that maintain trust [2].

In the last decade, the infrastructure of Information Communication Technology has seen huge changes in the way it operates. Modern ICT ecosystems utilise the connection of multiple devices and services, all with the capability of processing and storing large streams of "Big Data" in real time, enabling a process known as data analytics [61]. Data Analytics affords the users' ability to identify future trends or establish strategic plans using large streams of data [61]. Furthermore, developments such as the Internet of Things, enable everyday devices that were previously known to be "Dumb" to become "Smart", as built in sensors enable users to control or display current settings of each device. The added connectivity of such developments is sure to add complexity in legislating data transactions, as disputes surrounding data ownership, jurisdiction over cross border transactions and regulating organisational use of such technology occurs [62].

Regulators, Policy developers and Information Commissioners, have a huge task ahead of them ensuring that such innovations are not abused [2]. Evidence presented by Edward Snowden highlights that government agencies actively attain user data without consent and perform covert surveillance on the population [63]. The same can be mentioned about some organisations such as, Facebook, which has been guilty of selling personal user data to third parties without the data subject's consent [64]. These issues have been addressed by data protection laws and Facebook has since updated its user agreements specifying the ownership rights of personal data, but these are just examples of actions that devalue trust between consumers and governments or organisations and establish a negative public opinion of technologies [65].

One application that the public remain fearful over is Biometrics. Despite the large interest shown in utilising this technology to improve existent identification and authentication fields, particularly for national security interests [65] many remain sceptical about the use of such technology deeming it as privacy invasive. The relationship between biometrics and privacy has long been at odds since its inception [65]. While some shareholders such, as governments and organisations state its effectiveness in speeding processes,

protecting the public in matters of national security and even complementing privacy. It is believed that installing clear guidelines and enforceable regulations can help address such concerns, enabling each stakeholder to experience the economic and social benefits of the technology without sacrificing privacy [66].

A. Organization

This paper provides a comprehensive review of the privacy concerns raised with the development and use of biometric technology. The paper intends to explore three separate, yet intertwining issues:

1) The history of biometrics, its modern uses and capabilities.

2) The privacy concerns brought by biometrics.

3) The effectiveness of current data protection legislation and policy administration in within the European Union and United States to understand shortcomings and best practices.

II. WHAT ARE BIOMETRICS

A widely used definition of biometrics is 'a system used for authenticating or verifying and identifying an individual, based on of their physiological, behavioural and biological traits' [3].

Traditional biometrics such as fingerprint systems applies pattern recognition techniques for Identification [4]. One method of identification is authentication, used to confirm the identity of an individual. It may be used in a scenario where a source of biometric data is captured and a comparison is made with the existing stored data of that person. This type of identification is commonly described as 1:1 matching [5].

These systems are commonly used in Banking Solutions, smart phones as well as public service delivery systems such as, health care and pension schemes [6]. The alternative to this is identification and verification, this method is used to match biometric data of an unknown identity with all pre-existing biometric data available in the database [4]. Verification and identification are commonly described as 1:N matching in this type of system the number of comparisons is determined by the amount of users within the database. Many organisations incorporate biometrics for verification and identification, for example, it is used in systems to ensuring national security, public order or for workplace time management systems [4].

In addition to this 'biometrics is an automated recognition tool that permits one to recognise when their dealing with known or unknown individuals, and subsequently note whether they belong to a group with certain rights or a group denied of certain privileges' [7]. Biometric systems offer the ability to identify individuals, control access to physical spaces, services, data and other benefits, as well as controlling the movement between international borders.

A. First Commonly Known Adaptation

The usage and concept of biometrics, has been around for centuries, with the first documented implementation in 14th century China, where fingerprints were used for identification. This was followed by another major development in 1901, when the Assistant Police Commissioner Sir Edward Richard Henry established a fingerprint database known as the Metropolitan Police Fingerprint Bureau. This database was then used to prevent criminals from successfully disguising their previous convictions from law enforcement, courts and prisons [8]. As time has progressed, new threats have surfaced and governments have reshuffled their approach. The rise of criminal and terrorist acts is believed to be the driving force in the decision for governments to redevelop surveillance systems and create new solutions [9]. It is suggested that the 9/11 bombings where the catalyst to the large-scale deployment of biometrics, as governments pursued quicker more accurate measures of verifying individuals to prevent further terror attacks occurring [10].

B. Evolution of Practices

Throughout the last decade biometrics continued to develop, as researchers aim to maximise the capabilities of identity management systems due to demand. Together with the aid of technological advancements, they developed more accurate and efficient systems suited to a variety of modern day applications [6]. The implementation of biometrics throughout society has rapidly increased as organisations seek efficiency, reliability and security; this has resulted in passwords slowly being replaced.

The most significant developments in biometrics are SOFT, GAIT, Bio modal and GAZE, these techniques have aided in expanding the range of methods for identification techniques. Individuals can now be identified based on intrinsic traits that are unique to them [11]. These techniques are based on characteristics such as, the way they walk, their vascular patterns, blood circulation, vocal chords, their DNA genetic makeup and shadow. Furthermore, the fusion technology employed in bimodal biometrics enable multiple traits to be combined which further increases accuracy and security of identification in methods. The versatility of biometrics has resulted in a widespread uptake of the technology. Furthermore, education and childcare facilities are implementing biometrics to ensure that children are in an environment where only authorised persons can gain entry [12]. Many governments employ identification systems with uses such as The National Identification in India and electronic passports in Germany. This also extends to many African countries such as Nigeria, Zambia, Malawi, Rwanda, Ghana and Senegal, which have invested heavily in biometric systems during elections to ensure that voting remained fair and free from corruption [13]. The health industry has also benefitted from biometrics, as Gold reports that the United Kingdoms, National Health Service employs a biometric Single Sign-on system to allow clinicians and other staff to authenticate themselves at the start of their shift, whilst the United States (US) opt to use it to detect patients that pay for healthcare and illnesses that they experience [9]. Interestingly, a company named Neurotechnology reports that it has successfully implemented biometric identification and object tracking technology into surveillance systems. An application entitled Sentiveilence 4.0 enables real time object identification and objects classification and can accurately track objects, vehicles and pedestrians, the system is more than capable of supporting security and surveillance applications as it can match the biometric face images against internal databases, such as criminal watch lists, with great accuracy and speed relative to

traditional systems. An alert may then be triggered instantaneously according to requirements [14]. Such systems have been deployed to identify criminals amongst festival goers with notable deployments at the Download Festival that was held in Leicester in 2015 and the Notting hill Carnival in 2016 [15].

One of the more recent developments in biometrics is the usage of Electroencephalography patterns. (EEG) patterns can be used to track brain waves, which may be used to Secure Vehicles and prevent hijackings through verifying the drivers' identity. Furthermore, EEG patterns may be used to identify the drivers' ability behind the wheel, identify their level of tiredness or sobriety. The system functions through checking the users' current EEG profile against their normal profile to determine if you are fit to drive [16], [17]. Another interesting development is Advanced Persistent e-Biometrics. This new phenomenon can be used to secure an individual's computer system by utilising advanced keystroke algorithms, which can extract the users' digital imprint through their interactions with a keyboard. The system continuously verifies the user's identity through identifying them through the way they type. The algorithm analyses the speed of typing, time spent pressing keys, and the most commonly used capital letters, this information is then stored as the user profile. Once the users profile has been accurately identified, the profile may be accurately compared to the incoming keystrokes to determine in real-time whether the user is who they claim to be [18]. Typewatch is a commonly used e-Biometrics solution that operates through continuously monitoring identity of data theft attempts by analysing text typing patterns of each user [19].

III. Privacy

The concept of privacy is difficult to define, as customs of association and disassociation are cultural and relative to species [20]. Entering a house without knocking on the door may be considered a violation of privacy in one culture and acceptable in another [21]. The term privacy is used in many political and legal discussions yet very few can give an exact definition to accurately define it. However, since many of its definitions overlap and many laws share similarities, one way to possibly understand the concept would be to trace its iterations historically whilst noting the small differences in definitions.

One of the earliest definitions of privacy is by Westin who describes the term as [22] the "right to control, edit, manage, and delete information about one's self, deciding when, how, and to what extent this information is communicated to others". Additionally, Parent maintains that privacy consists of a form of sovereignty over private matters [23]. Recent research quoted by [21] further updates Inness's definition of privacy as "the state of possessing control over a realm of intimate decisions, which include decisions about intimate access, intimate information, and intimate actions".

This paper argues that the definition of privacy poses a great challenge to scholars and researchers, which consequently makes its application evermore challenging. Problems are presented while defining matters relating to a person's innermost self, as explicitly describing this area remains an elusive task. Therefore, a resolution can be made that each notion of privacy is relative to culture and reliant on factors such as economics and most importantly technology available in a cultural region [24].

IV. Biometrics and Privacy

The motivations for using biometrics are diverse and often overlap [25]. The uses include improving convenience and efficiency of routine access transactions, reducing fraud, enhancing public safety and national security. However, many argue that biometric technology has become more intrusive to privacy than ever before, as its use creates widespread debate across many important key figures [26]. The adoption of approaches such as GAIT and SOFT creates the idea of a surveillance society amongst users, where individuals are no longer able to roam streets with a level of anonymity. The accuracy afforded in these approaches and the versatility of its application pose key questions regarding privacy.

A. Key Issues

The following figure (Fig. 1) presents a survey conducted by FIND Biometrics on experts in the Identity Management industry. It helps reconnoitre the challenges faced in biometrics systems today [27].

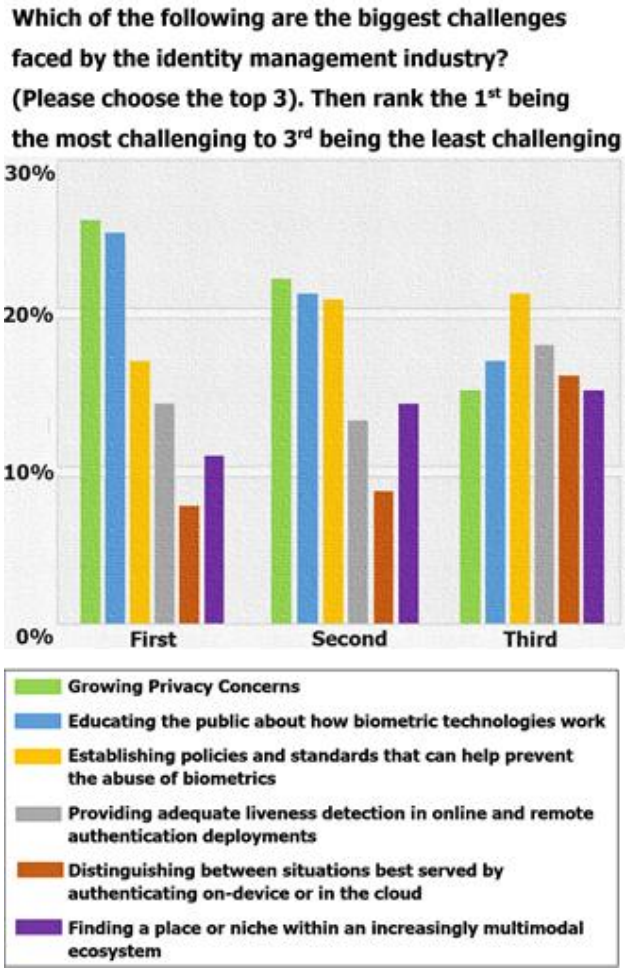

Fig. 1. The Biggest Challenges in Biometrics, 2015 [27].

1) The most challenging issue identified was growing privacy concern. Results pointed to the failure to incorporate privacy in the design of products.

2) The next issue was educating the public about how biometrics operate. Some researchers noted that privacy concerns existed due to lack of understanding on biometrics, educating the public is one ensures they understand basic security principles.

3) Finally establishing policies and standards that can help prevent the abuse of biometrics is noted as a challenge. Creating these may help in overcoming the first two challenges and may further aid to restore public trust in it is application.

The House of Commons published a report that aimed at identifying the current and future uses of Biometrics in the UK. In response to the Government silence in disclosing its biometric strategy, the report details a list of risks associated with biometrics [28]. Once these risks were identified, a scenario was presented for each risk detailing a possible application that could affect the privacy of a data subject.

The following key privacy concerns related to biometrics where illuminated:

1) Biometrics may be used as a method of locating individuals. Since biometric data is unique, it holds potential to track individuals physically as they access facilities or have their biometric traits documented by surveillance systems. Notably an individual may be tracked during each interaction with a biometric system. Each separate interaction can be linked to enable complete surveillance, which may infringe upon spatial privacy. There are growing concerns that Governments may exploit such systems, for example in China the increased tracking of citizens by police, creates fears that police have the ability to monitor political and religious dissidents, and that the information may be used to target or detain certain groups [29].

2) The inability to assure users that biometric data is stored safely and transmitted in a manner that preserves privacy. For instance, the notion of storing biometric data in a central database raises privacy concerns, as there is only one single point of failure. A mobile phone with a weak storage database may allow the biometric template to be captured before storage and subsequently stolen [30]. Furthermore, disparity between data compliance has resulted in unsecure data transmission, as highlighted by Safe Harbour agreement where The United States Of America infringed upon the terms set by the EU commission, which enabled the United States to intercept and interpret data that was transmitted [31].

3) Biometrics may enable function creep, which describes a situation whereby biometric data that was previously collected for a specific purpose is later used for unauthorised or unintended purposes. Function creep occurs when technologies are installed without the formulation of guidelines to monitor their operation resulting in shareholders using information to their own benefit [30]. Many new fitness watches contain a wealth of medical data. It has been note that earlier versions allowed insurance companies, and the health department to obtain this data and actively discriminate using the details [32].

4) When, the use of biometrics violates the "principle of proportionality" that states climatic data should only be used when acceptable, relevant and not excessive to the goal of the system.

5) The collection or sharing of biometric data without the consent of the user, adequate knowledge given or notice with a specific reason.

6) The use of biometrics for purposes other than the one agreed upon or misuse to further generate extra information.

7) Points 4, 5 and 6 can be better described with the following scenario, the Walt Disney resort use biometric fingerprints to prevent customers from redistributing their tickets. The new scheme now uses biometrics in the form of a facial scan or fingerprint to verify annual and multiday passes. Many users have stated that they were surprised when visiting the resort when they were told that their fingerprints would have to be taken. Many have stated that no information was provided prior to their visit about the biometric system and that they would be required to give fingerprints [33]. Leading privacy groups', as well as, the Electronic Privacy Information Centre to state that such an act is a "gross violation of privacy rights" and the principle of proportionality as customers don't receive information regarding how their biometric data is collected, how it is used and the protection afforded to the data. It has been noted that Disney's facial recognition subcontractor, Identix has contacts with the US government and some claim to have strong evidence that can rectify that the two entities do correspond with each other on numerous projects; that the Department of Defence utilise biometric information obtained by Disney in its renowned fingerprint system [34].

8) Since biometrics utilise biology to identify individuals they hold the ability to reveal an individual's ethnicity, gender or sexual orientation. The fear here is that this information may be used by organisations as a method of discrimination. Systems such as the biometric facial recognition may display critical information that enables banks to identify consumers of importance may be given more priority, any nuisance protests can be prevented early on, as protestors can be identified at the assembly point [35].

9) Most organisations share a discrepancy in having an inability to clearly define to users how long they will retain their biometric data. Keeping data too long can give opportunity to misuse, allowing function creep to occur as information may be sold on. Prior to the Protection of Freedoms Act 2012, law enforcement in the UK were permitted to retain biometric data obtained from suspects as long as they saw fit [36]. However, under the Protection of Freedoms Act, biometric data that is obtained from individuals that have been arrested or charged for minor offences must be destroyed following a decision not to charge the individual or

an acquittal. If charged for a serious crime but not convicted Biometric data is retained for three years before deletion [37].

*10)*Another problem introduced in biometrics is the copying and removal of biometrics from the original use to secondary purposes. Governments and private companies tend to gather this data for secondary uses [38]. Nagar explains that unique identifiers in biometric templates can be reused across databases without the production of a new biometric sample. Subsequently this allows unrelated databases to pull templates from their original database for identification in a different system [39]. Australian law enforcement has stated that it hopes to develop a national biometric system that draws upon pictures from social media sites to build a national database. Social media sites will be required to share data upon request of law enforcement. This has sparked uproar amongst privacy groups who argue that privacy is forcibly removed from an individual, however law enforcement state that privacy impact assessments will be drawn up to offer more transparency over the usage of biometric data [40].

B. Identifying Concerns from a EU – US Standpoint

The Commons Report attributes the failures in the governance of biometrics, to the rashness into adapting the technologies aiming to benefit from the tools, without interpreting the risks that they can bring to society [28]. Such instances can be seen in the failed border identification scheme, the problematic police DNA, fingerprint retention and disposal practices which have since seen reform with the introduction of the Protection of Freedoms Act. Furthermore, the governments delays in publishing its Biometric Strategy is deemed rather worrying and as failures to explain its usage of the technology and its methods of handling the issues related to the technology, means that governments lose the opportunity to be transparent and reassure the public the applications can be controlled [41]. Gellman asserts his findings over those identified by [28]. The author uncovers approaches that utilise fair information principles to balance the outcome, offer transparency and protect privacy. In the report, Gelman adds that legislation can also be responsible for some of the risks that can be found in applying biometrics. Such problems include failures to provide clear definitions, as to what constitutes to personal information and adequate protections such as mandatory rules regarding prior consent and notices before collection or processing data. Such measures are especially important when applied to specified international organisations and countries that wish to process, transact or utilise personal data of individuals from one country, but do not offer the same level of protections as the country that the individual resides in, subsequently leaving these individuals at risk. A prime example is the nullified Safe Harbour scheme. Which was an extensive agreement between the US and EU, used to bridge the differences between the regulatory regimes and allow data to be safely transferred between nations while ensuring the preservation of data protection. Oversight was discovered in the agreement, which allow for US organisations to inadvertently access the data which led to the end of the scheme and the establishment of a replacement mechanisms which has come to be known as The EU/US Privacy Shield agreement [30].

The EU/US Privacy Shield agreement aims to provide stronger privacy protection and oversight mechanisms. Furthermore, it will enable multiple redress possibilities and present new safeguards directly related to US governments' access to personal data. United States organisations that wish to transact data will now have to self-certify according to the standards set by the Privacy Shield. The European Commission would then conduct periodic reviews to assess whether the level of protection provided by the Privacy Shield remains adequate. To show its commitment in establishing transparent mediums with the EU the United States will cooperate with Article 29 Working Party, regarded an important data protection stakeholder in Europe. This partnership aims to ease concerns over commercial and national security aspects of the Privacy Shield agreement [30]. Mordini and Petrini [42] add valuable points to the ones made by [28], [30] and approach the subject of privacy concerns from an ethical and social standpoint. They argue that since biometric templates contain information that can be used to identify an individual, more must be done to ensure that the devices do not infringe human rights and only work to their agreed functions. The hope is that by upholding civil liberties the devices may be able to limit the extent at which governments and organisations can exploit the technology [42].

Such was the case with Google. Rivera v. Google Inc., No. 16 C 02714, a class action lawsuit that relates to the unlawful scanning of faces in photographs described by the Illinois Biometric Privacy (BIPA) [43]. Naker and Greenbaum [43] identify that this class action lawsuit filed against Google significantly highlights, how organisations can abuse individuals' privacy if they have the tools to achieve this. Furthermore, it also highlights matters of jurisdiction and questions about the definition of a biometric identifier under BIPA. BIPA provides strict data protection, pertaining to notice and consent requirements on organisations. It also adds a definition of biometric information, prior notice, consent and restrictions for biometric identifiers and biometric information. The lawsuit brought before the district court alleged that Google violated BIPA by collecting the plaintiffs biometric information from photos that had been uploaded to googles' photo sharing and storage service without prior consent, following which Google failed to publish information relating to the data retention and destruction schedule. Google argued that BIPAs' regulations did not apply to the case as, actions took place outside of Illinois and the facial templates created using the photographs did not constitute to biometric identifiers. A federal district court in Chicago has since rejected Google Inc.'s motion to dismiss stating that physical traits gleaned from photographs are covered under BIPA. This case highlights the successful application in providing and enforcing protections for personal data. However, the most troubling finding according to Naker and Greenbaum was the state of governance in The United States, which offers fewer and less effective data privacy protections than the EU. [44] The United States Government Accountability Offices' (GAO) report, identifies and reviews relevant academic studies, congressional testimony, position papers, reports from federal agencies, privacy advocates and documents from industry stakeholders to identify current privacy Issues, and Applicable Federal Law for facial recognition technology. GAOs report

finds that very few US state laws apply to biometric data or manage to clearly address the key privacy issues raised by stakeholders, for example specifying the circumstances where the technology can be used to track or identify the whereabouts of individuals. Finally, GAO suggests changes to the current consumer privacy framework with the aim of reflecting the effects of rapid changes in technology and the marketplace in a better way, and also to solve the privacy issues raised by stakeholders [45]. To add to this Georgievas' research into privacy and the legality of foreign surveillance uncovers that the United States Constitution does not specify privacy as a human right which triggers the question; what constitutes to a human right and what then constitutes to a violation [46]. Deeks adds that the United States tend to put national interest ahead of privacy with the nations combined safety having higher precedence over an individual's privacy. Deeks later demonstrates this through relating the legislation stating that the rights of data subjects begins to blur when matters of terrorism occur. Carmi [47] offers a comprehensive study into model for assessing freedom of expression among Western democracies the author states that privacy laws in the United States are often based on liberty values. As social anxieties focus principally on government institutes and police, and are based on concepts of liberty. On the other hand, [47] states that the European Union's approach to privacy laws are based on instilling dignity which relate to the universal rights of a human being that cannot be infringed under any circumstances. Tzanou [53] adds to this argument stating that the differences in each nation's privacy regimes can have a negative effect on transborder dataflow transactions as displayed by the nullified Safe Harbour scheme. Tzanou further adds that the war against terror can also pose a threat to civil liberties and subsequently affect the privacy of citizens. Further stating that [52], since the databases afforded to governments and organisations have the ability to store vast amounts of data, there is a possibility that surevilance networks become interlinked and databases are used to track individuals. Tzanou states that such systems already exists, for instance, the EU-US Passenger Name Record (PNR) agreement, which enables EU-US sharing of passenger details, in an aim to tackle threats to national security. Tzanou raises two key concerns: the first being that, despite the EU and the USA agreement to respect each other's data protection laws, past events dictate that such an agreement will not be without difficulties as the privacy regimes offer vast differences. The second concern is that the EU states that it aims to implement similar surveillance schemes to that of the US to combat terror. Tarrow [55] states that since the EU and US employ very contrasting privacy regimes. An EU approach to surveillance, similar to that of the US would infringe the human rights laws afforded to all Europeans under the European Convention on Human Rights and the Data Protection Directive.

The following section aims to uncover the current structure the European Union and the legislation used to manage the personal information in the EU. After this, the papers will issue that may infringe the effective application of privacy. Then finally, solutions that may ease concerns and ensure effective governance of biometrics will be illucidated.

V. PRIVACY LAWS & STANDARDS

The official structure of the European Union is described by the European Commission in an official guide, where it identifies the most important actors involved in the data legislative process [49].

The structure is as follows:

- The European Parliament – is composed of members who are elected every five years by the people in each Member State.
- The Council of the European Union – The Council is composed of ministers who represent the Member State governments.
- The European Commission – The Commission Acts as the central administrative structure of the EU, it is involved in most fields of action.
- The European Data Protection Supervisor - role is to protect citizens' personal data processed by the EU institutions and bodies.
- The Court of Justice of Europe - It ensures EU law is uniformly applied in each EU country in the exact same manner as it is written; actions can be taken against EU countries that do not conform to appropriate data protection.

Bartolini and Siry [48] states that the most important figures within the data protection legislative process are, The European Data Protection Supervisor, The Court of Justice of Europe and the Article 29 Working Party, which gives guidance and recommendations to the commission on methods of protecting data.

Bartolli and Muthuri [49] specify that Europe's motion to reform its data protection legislation from the Directive 95/46/EC to The General Data Protection Regulation (GDPR) is because it had to build legislation capable of handling the governance of developments such as the Internet of Things and Big Data. The GDPR is set to come into effect on the 25 May 2018 and will replace the DPD. Additionally, the GDPR will extend the reach of EU data protection laws, focussing on data controllers and processors that collect, process or transmit personal information from EU residents.

It is a requirement that each member nation applies the legislation passed by The Court of Justice of Europe (CJEU) into their National Law, to be considered as compliant. [50] Furthermore, the GDPR is explicit in explaining conditions that constitute safe practices in handling and processing personal data, sensitive data, consent, regulatory powers and individual rights. As identified by Mordini, European law is often based upon human dignity, this can be demonstrated in the continents approach to governing organisational uses of data [47]. This is illustrated in the EU Charter of Fundamental Rights and European Convention on Human Rights, which effectively enshrine personal data protections, transparent administration and guarantees of bioethics as basic human rights for any individual within Europe [51]. Bustard [52] studies the impact that the Reformed EU privacy legislation could have on Biometric system deployments, adding that the GDPR

interprets raw biometric images or templates as personal data, and regards the processing of biometric data to uniquely "directly or indirectly" identify an individual as sensitive. Article 9(2) of the GDPR explains the few conditions where processing sensitive personal data can be permitted. Furthermore, due to revelations of data surveying and failures in transborder data flows, the CJEU will extend its jurisdiction, enforcing the same personal data regulations on non-EU organisations that monitor or process personal data or offer services to EU Data Subjects. Additionally, Article 9(4) of the GDPR will enable EU Member States to impose or maintain further conditions with regard to the use of biometric data. The European Commission reports that biometrics has the potential to interfere with human rights, liberty, intimacy, human dignity and privacy. Therefore, any use of a biometric system must comply with the European Convention on Human Rights and with the Data Protection Directive.

Bartolini and Siry [48] argues that although the GPDR provides clear guidelines and protections toward personal data; some doubts remain regarding its ability to govern the rapidly changing digital ecosystem, when it employs a broad structure that aims to cover all aspects of data processing. The ability to extend or reduce further conditions regarding the use of biometric data will be instrumental in helping govern such technologies as changes occur and issues develop. The GDPR is still somewhat untested by biometric applications, due to its recent development and implementation. However, its overall structure should enable effective governing as more pressing matters develop over the years.

VI. Remidiating the Problem

The House of Commons published a report based on 33 written submissions and 14 oral pieces of evidence [28]. From the compilation of evidence The House Of Commons states that the application of biometric technologies indubitably increases legal and ethical concerns associated with privacy, confidentiality, autonomy, informed consent and liberty. The values stated are not regarded as absolute but, are crucial in liberal democracies such as the UK, who strongly believe in not restricting them. The House of Commons suggests the use of the principle of proportionality when considering possible implementations of a biometric application, suggesting that this would enable a balance to be struck between societies need for a system and uphold an individual's rights. Kindt [56] adds to the argument stating that referencing that the principle of proportionality is currently employed within the GDPR. Furthermore, Kindt references a successful implementation by the European commission which challenged the United Kingdoms use of Biometrics in schools, arguing that the use of such a tool for the purposes of recording the attendance of minors was unnecessary, therefore the CJEU ruled that parental consent would be required prior to any installations of biometrics that identify minors, furthermore an alternative method of identification should be used.

However, [44] GAO suggest that based on findings from its performance audit of Facial recognition, the current privacy framework employed in commercial settings in the US requires reform. Additionally, GAO reports that despite the efforts from government agencies, industry trade organizations and privacy advocacy groups to develop guidelines base upon fair information principles. The guidelines remain plagued with issues as guidelines do not specify key information such as mandatory requirements of notification or consent. Technologies such as GAIT have the ability to accurately identify individuals at great distances, therefore organisations must identify how they can successfully tackle consent, for example in instances where facial recognition is used at the entrance of a building, companies must identify whether this is a valid approach. GAO adds that a large number of stakeholders suggested the approach of privacy by design as it would address consumer privacy at each stage of product development.

The Federal Trade Commission offers its support for Privacy by design initiatives stating this practice enables organisations to build systems only to its desired purpose and never beyond [57]. Once data no longer serves the original purpose it is deleted, which eliminates issues of function creep. Similarly, [25] Mordini signifies that collaboration and debate amongst developers, researchers and technicians will enable core concerns of biometric implementation to be elucidated and dignified approach can be taken when building the system from the ground up. The International Biometrics & Identification Association (IBIA) supports this claim stating that measures that allow segregation of data and the encryption of information [58]. However, GAO specifies that some industry representatives and privacy advocates believe privacy by design has considerable limitations, since some biometrics and facial recognition systems are built to be flexible and allow for users to change the privacy protection levels with ease as they see fit [44]. Such as design may possibly give the user the ability to bypass built in protections included in the system design, such as a data retention timeframe.

Geppert reviews the current the EU framework on transborder data transfers recognizing the importance in international collaboration for transatlantic commerce, specifically between EU counties, US, Canada, China and India [59]. After a thorough investigation the author concludes that cultural values can significantly impact the agreements and enable oversight. Consequently, the author states that the EU-US Privacy Shield offers an efficient model that could be used to form transborder dataflow collaborations with other nations. The author argues that a hybrid approach may offer the best solution. The mandatory baseline requirements of a privacy shield collaboration could be extracted into a self-certification scheme. Each country that meets this standard would then collaborate with the commission to establish the main body of the agreement. This approach incorporates the interest of both parties and ensures all parties are knowledgeable with regard to the stipulations.

Leicester and Kulkarn [60] identify a different approach to possible transborder data flow collaborations for biometric technologies. After an extended review of current privacy concerns, the different philosophies, and approaches taken by stakeholders of biometrics. The researchers conclude that due to the successes in legislating privacy in Europe, a Global Biometrics Commissioner should be developed. This commissioner would run similarly to the EU commission. Structurally it would act as a central hub independent of any

government and trade organization, its role would be the development of policies and enforcement of penalties. Any organization or government that uses biometrics would have to comply with the policies established by the Global Commission. In developing this practice, the author hopes to provide a solution that adopts the core values of the European Union and effectively instil them across each application of biometrics.

The United States Government Accountability Office states that organisations such as International Biometrics and Identity Association (IBIA), the European Commission, OECD and representatives of other continents must work together to effectively bridge the gap between all shareholders, due to their ability to bring governments, policy makers, manufacturers and organisations together to offer advice on the use of biometrics and implementation of privacy [44]. Furthermore, such organisations may propose frameworks to address challenges and campaign for "open governments" that offer transparency and participation during regulation to ensure regulation serves public interest.

The Ireland Bioethics committee further compounds this by stating that for privacy and biometrics to go hand in hand it is essential that consideration is taken when implementing a biometric application to determine whether the application is necessary and can be justified. It is vitally important to weigh societies need for applications that combat terrorism or fraud against for individual rights and liberties. Through the principle of proportionality, a balance can be struck between individual's rights and societal interests. This may effectively ensure that each biometric application balances the rights to privacy of the involved individuals [54].

VII. Conclusion

The implementation of the next generation of biometrics could inadvertently affect the privacy of billions of people worldwide. Due to the versatility and high accuracy afforded to the technologies, many governments and organizations are adopting these applications. However, their lack of transparency and failures to define and properly govern biometrics could cause the loss of civil liberties and tarnish human dignity. Problems begin when defining privacy, as the meaning of privacy differs for every individual according to their cultural values or geographical location. This can be demonstrated by US approach to governing privacy laws focusing on liberty values and security over privacy and anonymity whereas, the EU focuses on human dignity, encompassing the respect of the human being. However, privacy advocates, worry that these approaches in relation to biometrics and privacy, often favour the governments and organisations, allowing for abuse of powers subsequently leading to loss of privacy, ambiguities in legislation and a lack of transparency. The EU approach is welcomed by privacy advocates, due to its recognition of personal information as a human right, which then drives many of its data protection laws. The EU has successfully challenged member states such as the United Kingdoms', use of biometrics in schools. Such actions signify its interest in holding governments and, organisations accountable and championing the protection of privacy. Furthermore, the EU has also made great progress with trans-border agreements which has led to many stating, that the EU-US Privacy Shield can be used as a hybrid model that could potentially solve the huge problems faced with trans-border data flows between countries counties that offer different levels of data protection to agree on some common values and principles. However, despite these huge advancements, concerns remain regarding the use of biometrics, as many governments and organisations actively use it method of surveillance or for illicit monetary gains, causing uproar amongst the public. In light of this information, few resolutions can be made to tackle these concerns; Firstly, governments, law enforcement and legislators must work in tandem, offering transparency regarding their practices and if they can not disclose specific details, then they must explain how they will assure the maintenance of citizens' privacy during the operation of their applications. Secondly, stakeholders in Government, trade organisations, developers and legislators must come together and understand learn how new innovations in biometrics may be used, the versatility that each application possess and to what extent they can infringe personal information. Only then can guidelines be established that better suit the application of biometrics and uphold the rights afforded to the citizens.

References

[1] Nissenbaum, H. (2009). Privacy in context: Technology, policy, and the integrity of social life Stanford University Press.

[2] OECD. (2015). Digital security risk management for economic and social prosperity Organisation for Economic Co-operation and Development.

[3] Chauhan, S., Arora, A. S., & Kaul, A. (2010). A survey of emerging biometric modalities. Procedia Computer Science, 2, 213-218.

[4] Tripathi, K. P. (2011). A comparative study of biometric technologies with reference to human interface. International Journal of Computer Applications, 14(5), 10-15.

[5] Pal, S., Pal, U., & Blumenstein, M. (2014). Signature-Based Biometric Authentication. In Computational Intelligence in Digital Forensics: Forensic Investigation and Applications (pp. 285-314). Springer International Publishing.

[6] Unar, J. A., Seng, W. C., & Abbasi, A. (2014). A review of biometric technology along with trends and prospects. Pattern recognition, 47(8), 2673-2688.

[7] Pato, J. N., & Millett, L. I. (2010). Biometric Recognition: Challenges and Opportunities, Whither Biometrics Committee, National Research Council of the NSA.

[8] Corbion, P.A. (2013) biometrics: friend or foe of privacy? London, England: Privacy International. Retrieved from https://www.privacyinternational.org/node/245

[9] Gold, S. (2012). Border control biometrics and surveillance. Biometric Technology Today, 2012 (7), 9-11.

[10] Xiao, Q. (2007). Technology review-biometrics-technology, application, challenge, and computational intelligence solutions. IEEE Computational Intelligence Magazine, 2(2), 5-25.

[11] Zhang, D. D. (2013). Automated biometrics: Technologies and systems (Vol. 7). Springer Science & Business Media.

[12] Diffin, J. (2010). Delivering biometrics as part of a wider security infrastructure. Biometric Technology Today, 2010(8), 6-8.

[13] Nwangwu, C. (2015). Biometric Voting Technology and the 2015 General Elections in Nigeria. In Conference on The.

[14] Newton, J.A. (2015) SentiVeillance Provides Biometric Identification and Object Tracking for Video Surveillance Systems. Prweb. Available from: http://www.prweb.com/releases/2015/12/prweb13106156.htm [Accessed 22/04/2017].

[15] Martin, J.A. (2016) Notting Hill Carnival spycams: Met Police rolls out real-time live face-spotting tech. The Register.

http://www.theregister.co.uk/2016/08/26/notting_hill_carnival_police_surveillance_cameras_automated_face_recognition [Accessed 28/02/17].

[16] Nakanishi, I., Miyamoto, C., & Li, S. (2012). Brain waves as biometrics in relaxed and mentally tasked conditions with eyes closed. International Journal of Biometrics, 4(4), 357-372.

[17] Nakanishi, I., Baba, S., Ozaki, K., & Li, S. (2013). Using brain waves as transparent biometrics for on-demand driver authentication. International journal of biometrics, 5(3-4), 288-305.

[18] Teh, P. S., Teoh, A. B. J., & Yue, S. (2013). A survey of keystroke dynamics biometrics. The Scientific World Journal, 2013.

[19] OOSTDIJK, M.et al. (2016) State-of-the-Art in Biometrics for Multi-Factor Authentication in a Federative Context. Research ed: n/a. Available from: https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2016/201605-biometrics-english.pdf [Accessed 20/04/17].

[20] Moore, A. (2008). Defining privacy. Journal of Social Philosophy, 39(3), 411-428.

[21] DeCew, J. (Eds.). (2015) Privacy. The Stanford Encyclopedia of Philosophy, Available from: http://plato.stanford.edu/archives/spr2015/entries/privacy [Accessed 27/08/17].

[22] Westin, A. F. (1968). Privacy and freedom. Washington and Lee Law Review, 25(1), 166.

[23] Parent, W. A. (1983). Privacy, morality, and the law. Philosophy & Public Affairs, 269-288.

[24] Arndt, C. (2005). The loss of privacy and identity. Biometric Technology Today, 13(8), 6-7.

[25] Mordini, E., & Tzovaras, D. (Eds.). (2012). Second generation biometrics: The ethical, legal and social context (Vol. 11). Springer Science & Business Media.

[26] Adkins, L. D. (2006). Biometrics: Weighing convenience and national security against your privacy. Mich. Telecomm. & Tech. L. Rev., 13, 541.

[27] COUNTER, B.P. (2015) Year in Review 2014: The Biggest Challenges in Biometrics. [Online] FindBiometrics. http://findbiometrics.com/year-in-review-2014-the-biggest-challenges-in-biometrics-21211/ [Accessed 04/02/2017].

[28] HOUSE OF COMMONS, SCIENCE AND TECHNOLOGY COMMITTEE (2015) Current and future uses of biometric data and technologies. London: The Stationery Office Limited, 6.

[29] Keane, M. (2005). China's National Resident Identity Card: Identity and Population Management in Transition. *UCLA Pac. Basin LJ*, *23*, 212.

[30] LIU, N.Y. (2013) Bio-privacy: Privacy Regulations and the Challenge of Biometrics: Routledge.

[31] Weiss, M. A., & Archick, K. (2016). US-EU Data Privacy: From Safe Harbor to Privacy Shield. Congressional Research.

[32] POSEL, S. (2016) The Smart Tech Toys That Can Tell On You. [Online] https://occupycorporatism.com/the-smart-tech-toys-that-can-tell-on-you/ [03/02/2016].

[33] WOLF, N. (ed.) (2015) The new totalitarianism of surveillance technology.TheGuardian, retrieved from: https://www.theguardian.com/commentisfree/2012/aug/15/new-totalitarianism-surveillance-technology.

[34] Vacca, J. R. (2007). *Biometric technologies and verification systems*. Butterworth-Heinemann.

[35] CHABROW, E. (2011) Facial Biometrics Pose Privacy Woes. [Online] http://www.bankinfosecurity.com/interviews/facial-biometrics-pose-privacy-woes-i-1231 [Accessed 03/05/2016].

[36] Campus, R. (2016). *A critical analysis of US and UK legislation in the protection of civil liberties* (Doctoral dissertation, The University of Westminster).

[37] Home Office, (2012). Protection of Freedoms Act.

[38] Zibran, M. F. (2012). Biometric Authentication: The Security Issues.*University of Saskatchewan*.

[39] Nagar, A., Nandakumar, K., & Jain, A. K. (2010, February). Biometric template transformation: a security analysis. In *IS&T/SPIE Electronic Imaging* (pp. 75410O-75410O). International Society for Optics and Photonics.

[40] MEDHORA, S. (2015) Facebook photos could be taken for use in national biometric database – officials. [Online] http://www.theguardian.com/australia-news/2015/oct/21/facebook-photos-could-be-taken-for-use-in-national-biometric-database-officials [Accessed 05/06/2016]

[41] Gellman, R. (2013). Privacy and Biometric ID Systems: An Approach Using Fair Information Practices for Developing Countries. Center for Global Development.

[42] Mordini, E., & Petrini, C. (2007). Ethical and social implications of biometric identification technology. Annali dell'Istituto superiore di sanita, 43(1), 5-11.

[43] Naker, S., & Greenbaum, D. (2017). Now You See Me: Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy. BUJ Sci. & Tech. L., 23, 88.

[44] UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE *(2015) FACIAL RECOGNITION TECHNOLOGY*: *Commercial Uses, Privacy Issues, and Applicable Federal Law*. 15. Washington: GAO, 621.

[45] Georgieva, I. (2015). The Right to Privacy under Fire Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR. Utrecht J. Int'l & Eur. L., 31, 104.

[46] Deeks, A. (2014). An International Legal Framework for Surveillance.

[47] Carmi, G. E. (2008). Dignity versus Liberty: The Two Western Cultures of Free Speech. BU Int'l LJ, 26, 277.

[48] Bartolini, C., & Siry, L. (2016). The right to be forgotten in the light of the consent of the data subject. Computer Law & Security Review, 32(2), 218-237.

[49] Bartolini, C., & Muthuri, R. (2015). Reconciling data protection rights and obligations: An ontology of the forthcoming EU regulation.

[50] European Commission. (2012). *How the European Union works, Your guide to the EU institution*, Your guide to the EU institutionss. Luxembourg: Office for Official Publications of the European Communities.

[51] European Union. (2010). Charter of Fundamental Rights of the European Union. Official Journal of the European Union C83 (Vol. 53, p. 380). Brussels: European Union.

[52] Bustard, J. (2015). The Impact of EU privacy legislation on biometric system deployment: protecting citizens but constraining applications. IEEE Signal Processing Magazine, 32(5), 101-108.

[53] Tzanou, M. (2015). The War against Terror and Transatlantic Information Sharing: Spillovers of Privacy or Spillovers of Security. Utrecht J. Int'l & Eur. L., 31, 87.

[54] Donnelly, A. McMahon ,S. Sheikh, A,A. (2009) Biometrics: Enhancing Security or Invading Privacy? Dublin, Ireland: The Irish Council for Bioethics

[55] Tarrow, S. (2017). Close interaction, incompatible regimes, contentious challenges: The transnational movement to protect privacy (No. SP IV 2017-102). WZB Discussion Paper.

[56] Kindt, E. (2012). The Processing of Biometric Data. A comparative legal analysis with a focus on the proportionality principle and recommendations for a legal framework.

[57] Federal Trade Commission. (2012). Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies. October),(accessed March 5, 2017),[available at http://www. ftc. gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt. pdf].

[58] International Biometrics & Identification Association, Comments Submitted to Face Facts: A Forum on Facial Recognition Technology—Project No. P115406 (Jan. 31, 2012), accessed June 4, 2017, https://www.ftc.gov/policy/public-comments/comment-00074-3.

[59] Geppert, N. (2016). Could the'EU-US Privacy Shield'Despite the Serious Concerns Raised by European Institutions Act as a Role Model for Transborder Data Transfers to Third Countries?.

[60] Leicester, P., & Kulkarni, S. (2013). Investigating the Social Implications of Biometrics and the Need for Global Biometric Uniformity. International Journal for Infonomics (IJI), 6(1/2), 731-735.

[61] Rouvroy, A. (2008). Privacy, data protection, and the unprecedented challenges of ambient intelligence. Studies in Ethics, Law, and Technology, 2(1)

[62] Kshetri, N. (2014). Big data′ s impact on privacy, security and consumer welfare. Telecommunications Policy, 38(11), 1134-1145.

[63] Scheuerman, W. E. (2014). Whistleblowing as civil disobedience: The case of Edward Snowden. Philosophy & Social Criticism, 40(7), 609-628.

[64] Jamal, A., Coughlan, J., & Kamal, M. (2013). Mining social network data for personalisation and privacy concerns: a case study of Facebook's Beacon. International Journal of Business Information Systems, 13(2), 173-198.

[65] Nyst, C., Makin, P., Pannifer, S., & Whitley, E. (2016). Digital identity: issue analysis: executive summary.

[66] Box, S., & West, J. K. (2016). Economic and Social Benefits of Internet Openness