Investigating the Social Implications of Biometrics and the Need for Global Biometric Uniformity

Phillip Leicester[1] and Siddhivinayak Kulkarni[2]
School of Science, Information Technology and Engineering
University of Ballarat, P. O. BOX 663, Ballarat, Victoria, 3353, Australia

Abstract

This research paper looks at the social implications of biometrics pertaining to the ethics of privacy and the ownership of individual biometric data, including how these issues can be resolved through the establishment of a Biometric Commission by introducing global standardised biometric uniformity and the guidelines that will ensure their technological foundations. Much of the distrust that engulfs society is due to the past performances and policy implementations that governments have initiated surrounding biometric technology and its miss use beyond the realms of individual identification for security purposes. There needs to be total transparency from governments and organisations that use biometric technology for security identification in how every individuals biometric data will be used, stored and the ethical standards provided in eliminating many of the implications that every society has towards on how their biometric data will be used.

1. Introduction

The purpose of this paper is to examine the social implications and to a lesser extent the ownership of biometric material within the current technological world. By explain briefly what biometrics is and the application for which it is used for by governments, their agencies and of course various industries.

The fundamental intention of this research is to investigate and answer the question "Investigating the Social Implications of Biometrics and the need for Global Biometric Uniformity?" and to put forward my ideas on why the social implications of biometric material needs to be addressed more seriously by governments and businesses.

But more importantly through discussing the implications that biometric applications and their associated systems will have on society which concerns us all as they revolve around the issues of privacy, confidentiality, individual rights, ownership, transparency and accessibility to our own biometric data.

Furthermore, in undertaking the need for a biometric framework, a framework that will establish international standards for biometric applications and the systems that use such applications combined with the introduction of an independent body within every country that uses biometrics to oversee and ensure that the established international standards are maintained at all times, as well as regulated safeguards that are legislated to prevent the misuse of biometric material together with the implementations of procedures that will resolve the social implications that are associated with biometrics.

2. Literature Review

Biometric applications have been instigated by European and Western governments worldwide as a means to combat terrorism, asylum seekers, identity fraud and theft. Because of this biometric applications and their associated systems have developed continuously with advancements in technology, but what of the social implications that accompany these applications as stipulated by [1], [5] [4] and the ownership of the biometric material in question.

The social concerns identified with biometric data pertain to the issues of privacy, confidentiality, protection of data, individual rights, transparency, function creep and the collective rights between an individual. These are the areas that past research papers have focused on with some special attention paid to the issue of function creep, whereby information is gathered for one purpose and is then used for something entirely else without permission or knowledge of its use as mentioned by [2,1,5].

But what of the ethical issues and social implications that these applications provide in terms of data management and maintenance of ethical practices in dealing with disclosure aren't always adhered to [5] thereby creating a sense of mistrust and a lack of confidence throughout

society [2]. Biometric systems are used within many areas of industry and government for the purposes of storing data that are used by the system to conduct a matching process of our physical features based upon specific geometric points that rely on algorithms and clustering to provide an identification/verification of who we are.

According to [1] has stated within their research that the EU Commission has suggested within their working paper on data protection that the "purpose principle" must be respected at all times, in other words that the use of biometric systems should remain within the confides of the privacy act and as such no personal data shall be collected without any explicit and legitimate reason that justifies the need for such data. The "purpose principle" also refers to the removal of "function creep", a term that identifies the collection of data being used for one purpose, as well as being used for another without any authorisation whatsoever. As stipulated by [2] function creep installs a level of distrust and a significant lack of confidence that steps outside the ethical boundaries.

This is why there needs to be stringent guidelines introduced in addressing the social implications of biometric data, as well as policies that are continually updated in dealing with the ongoing technological developments involved with biometric systems and its applications. Then there is the problem of transparency, openness and accessibility mentioned by [4] whose research investigated the areas of the European Union policy associated with the problems confronting policymakers with freedom, security and justice. Maintaining a balance in formulating policies that identify the use of biometric systems/applications while upholding the rights of the individual isn't easy but it is a necessity as the legalities of our social freedom and democratic way of life cannot be hindered in any shape or form.

Other research undertaken by [8] claims that biometrics is aimed at reducing any risk or threat associated with terrorism by any individual, country, state or territory. This is somewhat of a misconception as no biometric system can distinguish who is or isn't a terrorist, unless of course known individuals have been positively proven to belong to a terrorist organisation or have themselves committed an act of terrorism.

Furthermore biometrics weren't developed to identify which countries, states or territories are associated or involved with terrorism for they are geographical land masses not human beings with unique biological features. And just because some individuals are of a particular ethnic culture doesn't by any means single them out to be associated with terrorism or to be illegal immigrants, for if biometric systems are used in such a way, then they have stepped beyond the legal and constitutional boundaries assigned to each and every one of us.

Her research [8] has also pointed out how biometrics differs between countries due to the lack of non-standardised global guidelines. For example the European Union defines biometrics as a measurement tool in determining physical characteristics, whilst the United States defines biometrics as being totally different from the European Union's definition. Instead the United States has decided to provide additional characteristics and behaviours to its biometric systems in order to undertake profiling of its citizens as well as other individuals of various groups. These differences amongst countries with regards to biometrics and their applications would remove many of the discrepancies through the introduction of global standardised biometric guidelines and policies established and implemented by a Biometric Commission.

Every researcher whose publicised research that was centred on the social implications of biometrics have all agreed on the need for transparency, protection, privacy and management of our biometric data and the need for stringent ethical standards to be maintained at all times by those who are responsible in using such systems. However, very few have nominated a proposal that would effectively address these vital and important ethical issues that confront all societies worldwide. Their analytical evidence does stipulate the need for concern when governments and security agencies start using biometric technology for profiling specific individuals of ethnicity which fundamentally erodes liberty and individual rights on a grand scale. The same applies to corporations who go beyond their authority in utilising biometrics for their own agendas that reduce the ethical standards of privacy and protection, as well as accountability.

Research has shown that there is a need to establish and implement global standardised biometric guidelines that will ultimately provide uniformity in collecting, storing, accessing, managing and using biometric systems, as well as upholding our privacy and individual rights associated with biometric sensitive data.

3. Social Implications

The use of biometric applications are becoming more prevalent in being used by governments, their agencies, as well as other areas of commerce/industry in obtaining positive identification/verification of individuals for the purposes of allowing access to high secure areas or to simply provide them with some form of ID.

Since the advent of September 11, 2001 governments worldwide have sort to use biometric technology as a political tool [5] in combating terrorism and cross border controls for which they

weren't designed for. There use by governments and national security agencies has created an ethical minefield in dealing with the social implications of this technology that affects each and every one of us. [4, 11, 12]

- *What of individual privacy?*
- *What about the protection of personal data?*
- *What the rights of the individual and those who use and store such sensitive data?*
- *How can society trust governments and their agencies to use their biometric data for its intended purpose?*

These are the questions that need to be addressed concerning the technology and those who rely upon its application. Our biometric data is sensitive information of our individual characteristics which requires highly efficient ethical standards of their use, so that such data cannot be used against us by those who seek to benefit from their disclosure to other parties without our knowing or our authority. Over the years those who were responsible for storing and accessing our personal information did so with a poor track record that failed to install confidence, but instead created distrust and cynicism. Such technology when used incorrectly by governments established a big brother structure that scrutinises every move that society makes as depicted in George Orwell's novel "1984". [5]

This is what we have to avoid and it can only be done when the implementation and use of biometric technology is completely transparent to all members of society by governments, security agencies and private industry that will install confidence and understanding through knowledge and education.

Philosophers are concerned about the "informisation" of the human essence as technology is proceeding to digitise our physical being, in particular where biometrics transforms us into patented products as a series of computerised digits that removes our very existence of who we are. As for civil libertarians their concerns with the use of biometric applications involves function creep, a term that refers to the collection of data that is used for one purpose, whereby that same data is totally used for something else without any authorisation whatsoever.[2, 13, 14] They have a right to be gravely concerned about "function creep" for it constitutes an evocation of our civil rights as individuals, as a society and for which our constitution was established to uphold including the constitutions of other countries as well.

The ownership of biometric data belongs to each and every one of us and as a result of this we the people are the only ones who can authorise the use of our biometric data. Those who collect and store our biometric data are the custodians whose responsibility is to protect such data and to obtain our permission for its actual use as stipulated within the privacy act of Australia, with the privacy acts of other countries varying somewhat.

The use of biometric applications does have a national and worldwide use, but not at the expense of the eradication of our social freedom and the rights that go with it in forming the fundamental fibre of all western democracies that were instigated by our forefathers.

4. Biometric Commission

In order to overcome the many social implications associated with biometric applications and there use, I propose the establishment of a Biometric Commission either in the neutral countries of Switzerland or Sweden with my preference being Sweden, whose sole responsibility will be to construct and implement global standardised guidelines on the development, implementation, management and security of biometric applications and their associated systems. Such a commission would operate similar to that of the United Nations or EU Commission as it would be totally independent of any government or political body and would consist of members from every country who are already using biometric applications/systems, as well as those who are just beginning to use such technology. Each country would also have an independent biometric ombudsman whose role will be to oversee the implementation of the commission's guidelines and to report any breaches of the guidelines, whereby action will be taken immediately. The commission will consist of philosophers, security specialists, researchers, international lawyers, academics and IT consultants whose appointment will be delegated by their respective countries.

The following diagram depicts the relationships and the flow of information between the Biometric Commission, other independent bodies, governments and their agencies, manufacturers and security agencies in adhering to the highest ethical practices and principles that will remove many of the current social implications with regards to the collection, use and protection of biometric data.

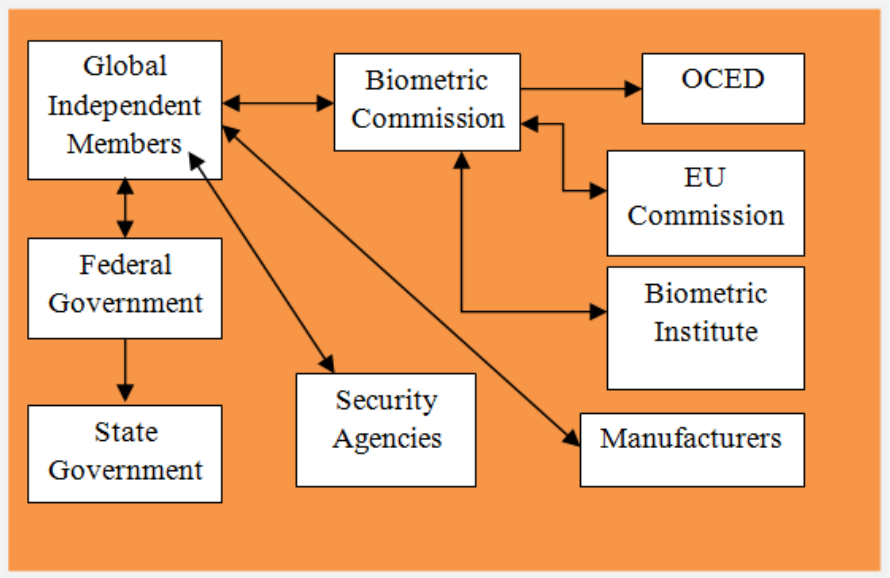

Figure 1. Overview of communication/information flow

- *Biometric Commission – An independent organisation responsible for the ethical establishment and implementation of biometric uniformity and policies.*
- *Global Independent Members – A member nominated by their country of origin in overseeing and upholding the policies of the Biometric Commission within their country.*
- *OECD – Responsible in utilising biometric uniformity for the designated protection of business organisations and that of social policy.*
- *EU Commission – Responsible for ensuring the Biometric Commission's biometric uniformity throughout the European Union.*
- *Biometric Institute – Engages in the implementation of biometric uniformity throughout the community by overseeing the ethical standards and responsible use of biometric technology.*
- *Federal Government – Collaborates with the Biometric Commission and implements their biometric strategy within federal policy.*
- *State Government – Engages with the Federal Government by implementing Biometric Commission strategy at the state level.*
- *Manufactures – Responsible for ensuring and implementing the development of uniform biometric devices that are globally compatible on all system platforms.*
- *Security Agencies – Responsible for the ethical operation, protection and storage of biometric databases.*

Much of what has been mentioned in establishing a Biometric Commission will conjure much debate, but it is a required necessity that other researchers before me to the best of my knowledge have not put forward a solution in addressing the social implications associated with biometric technology and their systems. They have merely outlined their concerns and the ethical implications that biometric systems will place on society.

5. Conclusion

Throughout this research paper in examining the social implications of biometric applications and their associated systems, have discovered the ethical issues dealing with privacy, protection, ownership, individual rights, transparency and operational use by governments, their agencies, security agencies and private organisations. All of these issues in whatever country have the potential to erode our freedom and civil liberties, invade our privacy and enable governments and corporations to use biometric technology as a means to establish a big brother environment that scrutinises our every move for which this technology wasn't meant to be used for.

This is a direct result brought about by the non-existence of global standardised guidelines as the

policies on the use of biometrics vary from country to country.

In establishing an independent Biometric Commission to investigate, establish and implement global standardised guidelines on the development, implementation and use of biometric technology and their associated systems would address and eliminate many of the social implications through installing and ensuring ethical principles of the highest standard.

Biometrics does have an important role to play in terms of our security, but not at the expense of eroding individual freedom and civil liberties or as a tool to single out certain ethnic individuals/groups based upon their cultural background, for that is too much of a price to pay. There needs to be total transparency and truthfulness regarding the implementation and use of biometrics to install trust and confidence in the technology, as well as the governments and corporations that use it, for then and only then will society seek to embrace it.

References

[1] Mordini, Emilio; Petrini, Carlo. (2007). Ethical and social implications of biometric identification technology. Vol 43. (1). pp5-11.

[2]Mordini, E; Massari, S. (2008). Body, Biometrics and Identity. Vol 22. (9). pp1-11. Oxford: Blackwell Publishing Ltd.

[3]Mordini, E; Green, M. (2009). Identity, security and democracy: The wider social and ethical implications of automated systems for human Identification. Vol 49, pp1-135. Amsterdam: IOS Press.

[4]Lodge, J. (2007). Freedom, security and justice: The thin end of the wedge for biometrics? Vol 43. (1). pp20-26.

[5]Ashbourn, Julian. (2005). The social implications of the wide scale implementation of biometric and related technologies. (pp 1-21). European Commission.

[6] Zureik, E; Hindle, K. (2004). Governance, Security and Technology: The Case of Biometrics. pp113-137.

[7]Pilgrim, Timothy. (2007). Biometrics and Privacy, pp1-22.

[8]Lodge, J. (2009). Biometrics: A challenge for privacy or public policy – certified identity and uncertainties. pp193-207.

[9]Alterman, A. (2003). "A piece of yourself": Ethical issues in biometric identification. Vol 5, p1. Netherlands: Kluwer Academic Publishers.

[10]Halperin, Ruth; Backhouse, James. (2008). A roadmap for research on identity in the information society. Vol 1. (1). pp1-17. Springer Publications.

[11]Sprokkereef, A; de Hert, P. (2007). Ethical Practice in the use of Biometric Identifiers Within the EU. Vol 3. (pp 177-201). Great Britain: A. B. Academic Publishers.

[12]Browne, S. (2009). Critical sociology. Vol 36 (1). pp131-150. Sage Publications.

[13]Michael, M. G; Michael, K. (2006). National Security: The social implications of the politics of transparency. Vol 24. (4). pp359-364. Wollongong: University of Wollongong.

[14]Smith, R. G. (2007). Crime control in the digital age: An exploration of human rights implications. International Journal of Cyber Criminology. Vol 1. (2). (pp. 167-179). Australian Institute of Criminology.

