IEEE-SEM, Volume 7, Issue 7, July-2019
ISSN 2320-9151

Privacy Concerns in Biometrics

EBELOGU Christopher U[(1)]., AMUJO Oluyemi E.[(2)], Adelaiye Oluwasegun I.[(3)], FAKI Ageebee S.[(4)]

[(1)(2)] Department of Computer Science, University of Abuja, Abuja FCT.
[(2)(3)] Department of Computer Science, Bingham University, Karu-Nasarawa State, Nigeria

* christopher@uniabuja.edu.ng

Abstract - Biometrics is any physical or biological feature that can be measured and used for the purpose of identification and authentication. Its features can be either physiological e.g. fingerprint, hand geometry, the face, the iris, the retina or behavioral e.g. voice pattern and gait (way of walking). The use of biometrics has seen an increase in the invasion of individual privacy due to security concerns. In this paper, we discuss the privacy concerns in biometrics and also provide some remedies to these concerns.

Keywords – identification, authentication, security, biometric, privacy, consent

Introduction

Biometric is characterized as an exceptional, quantifiable, organic trademark or characteristic for consequently perceiving or confirming the personality of an individual [1]. Biometric innovation is by and large progressively utilized as a part of ordinary exercises, for example, reconnaissance, time administration, enlistment of outskirt control, municipal rights, for example, voting, social rights, for example, human services and instruction (Biometrics: Friend or foe of privacy).

Biometric innovation has facilitated the utilization of passwords and token, biometric identifiers are utilized as a part of spot of passwords.

Numerous nations have embraced biometric advancements which have been implemented and demonstrated fruitfully. Cases are National ID frameworks used to avoid extortion and robbery, the savvy ID with the biggest incorporated circuit chip venture on the planet, the e-wellbeing frameworks which empowers simple access to medicinal services and lots more.

Biometric technologies are getting more consideration in the I.T world as well, in 2013 Apple added Smart ID to their I-phones, while most PCs we have currently either have the face recognition or unique finger impression scanner to logon to the pc.

Biometric Identification

Biometric identification is the procedure of coordinating a person to one of an extensive arrangement of framework clients [1]. The identification process compares a biometric, such as a fingerprint or a face recognition that is presented to the system, against all template entries in a database for a match [2]. This is alluded to as a one-to-many search. A one-to-many search seeks the matching identity of the offender; it is used to query number of entries in the database, until the result is matched. A 'one-to-many' hunt is utilized to *answer the question-who are you?*

Biometric Authentication

Authentication is a process where a known person's live biometric is compared to a stored template of that person [2]. Biometric Authentication verifies that the individual is who he or she claims to be [1]. An individual's identity is revealed to the biometric system upon entering a PIN (Personal Identification Number). To authenticate that this is the person associated with the PIN, a live biometric is presented by the individual and compared to the template and a match is determined. This is known as a 'one to one search'. It is more accurate than the 'one to many' application and is the predominant biometric process in place today and more privacy friendly of the two systems [2]. This answers the question-*Are you who you say you are?*

Biometric Functionality

Biometric functionality lists the desirable properties of a biometric identifier. The factors characterized by [3] are divided into seven (7) below:

1. **Universality:** Something that every individual has.
2. **Distinctiveness:** Can individuals be recognized in view of an identifier?
3. **Permanence:** How consistent is the identifier after some time for every individual.
4. **Measurability (Collectability):** Should be anything but difficult to gauge and not request an excess of time and costs.
5. **Performance:** Speed, exactness and robustness.
6. **Acceptability:** Willingness of individuals to utilize.
7. **Circumvention:** How simple is it to trick the framework.

What is Privacy?

In 1890, Warren and Brandeis popularized Judge Cooley's recommendation that privacy is the *'right to be let alone'* [4] and argued for the need for a legal protection of this right in the face of 'recent innovations and business techniques'. While the substance of the world and business strategies have changed, the Warren and Brandeis formulation remains one the simplest and most important response to the question of "what is privacy?"

Privacy is part of the claim to personal autonomy. It was stated at the 1969 Boyer lectures, that *"A man without privacy is a man without dignity; the fear that Big Brother is watching and listening threatens the freedom of the individual no less than the prison bars"* [5]. The importance of privacy is underlined by the fact that it is recognized and respected in different cultures throughout the world and it is protected in a multitude of national and international treaties, conventions and constitutions.

Biometrics Privacy

Privacy is a crucial human right even its absolutism is contested and in today's advanced world, it is the cornerstone that safeguards who are and supports our on-going struggle to maintain our autonomy and self-determination in the face of increasing state power. The Universal Declaration of Human Rights (12) and the International Convention on the Protection of All migrant Workers and Members of Their families (14) states "The right to privacy is upheld by an array of global and regional international human right treaties.

Biometric technologies can provide an accurate and rapid method of identification, thereby enhancing privacy and security – for example, by helping to secure personal information, by assisting an individual to retain control over his/her own information and by reducing the likelihood of identity theft [6]. However, the use of biometric technologies may also threaten an individual's privacy, and this technology has been criticized for its perceived Orwellian, invasive potential [7]; [8]. The use of biometric information raises concerns about the ability of an individual to control the information about him/herself that he/she is willing to make available to others, which would necessarily impact on his/her right to privacy. The privacy concerns related to biometrics are manifest in two spheres, those relating to personal privacy (i.e. fears about the erosion of personal identity and bodily integrity) and those relating to informational privacy (i.e. fears about the misuse of data and function creep).

Some of these uses appear to have the potential for greater privacy or enhancement to privacy than others. This debate has been occurring for many years and will continue until the public is satisfied with how implementations of biometric systems affect their private lives and protect their interests. Take for example, during Super bowl XXXV, appearances of fans were scanned and compared to mug shots of known criminals using a visual recognition technology. As you may envision, the reactions of privacy advocates were predictable, and right so [9]. However, the scanning was performed without the knowledge of the public, and utilized a methodology not fully understood for its impacts. According to Richard Norton, the executive director of the international Biometric Association, "The real perception problems come from passive technology that can be used without public knowledge".

The increasing use of technology and in particular biometric identification systems has not resulted in corresponding legislation and policy [10]. Safeguards must be set down for every step of the process from collection to retention with the right to privacy of individuals at the Centre. When collecting biometric data, individuals must be informed about the collection procedure, the intended purpose, and the reason why the particular data is requested and who will have access to their data. Beyond the biometric data itself, the physical or digital structure in which it is stored must be developed to ensure the safety of the data it

contains. If they are to be used, centralized mass data systems must be regulated by strict legislation in order to eliminate the possibility of the government or third parties(i.e. private sectors) taking advantage of the existence of the data for (new) unforeseen purposes.

The use of biometrics for authentication may have a low level of privacy risk provided that the authentication system involves the individual knowingly exercising a choice to enroll in a system and the system does not require the authenticating body to hold large amounts of information about an individual except that necessary to establish that the person is who they say they are. The use of biometrics for identification has the potential to be more privacy invasive in some cases; for example where it involves the identifying organization holding large amounts of information about individuals that it may or may not need, or that the individual may or may not know about. Other privacy risks arise regardless of the proposed use.

Personal Privacy

Our biometric information has the ability to "uniquely" identify us. Indeed, this specific feature of biometric information is one of the reasons that these technologies tend to evoke such heightened privacy concerns [11]. It was argued in [12] that, because biometric images facilitate our identification, we have a fundamental interest in controlling their creation and use, and that morally we have a greater interest in body-based information owing to the relationship between our body and our conception of self. Different experiences and interactions feed into this sense of self, which engenders a degree of complexity to each individual's personal identity. The ability to maintain and develop this complex identity is facilitated by, and is, thus, interconnected with, our possession of personal rights, such as autonomy, bodily integrity, and, particularly, privacy.

Informational Privacy

Many of the privacy concerns relating to biometric information can be distilled down to the ability of an individual to retain the control over this information and who has access to it. The philosophical foundations of the right to privacy would suggest that the loss of this element of control results in a loss of privacy. Moreover, the inability to control information pertaining to us also has negative connotations for the degree of autonomy, dignity and respect shown to us as persons [11].

- **Privacy and the Right to Anonymity:** Curtailing the concept of an individual's control over information relating to him/her, many people would prefer to keep their biometric (and other personal) information private and confidential and to only make it available to others on their own terms. An individual's right to privacy facilitates this ability to withhold personal information. By facilitating the ability to control availability of information about oneself, the right to privacy necessarily offers the possibility of anonymity. Furthermore, while it is accepted that in many situations an individual can rightfully be expected to identify him/herself, there is also an expectation of a right to anonymity and the freedom (autonomy) to make certain decisions (e.g. casting secret ballots in elections) and conduct activities during his/her daily life without always having to make him/herself known or to make this information known. In representing "something you are", biometric modalities enable the ascription of fixed identities to individuals. As a result, the proliferation of biometric technologies could further limit an individual's ability to remain anonymous and therefore maintain his/her privacy in particular circumstances, for example, with regards to political affiliations, religious beliefs or sexual orientation.

- **Collection of the Appropriate Information:** Notwithstanding situations where an individual wishes to remain anonymous, when an individual participates in a biometric programme, whether compulsory or voluntary, it is usually done so on the understanding that the information being collected will be used for a specified purpose. For many people, the lack of a definitive, specified purpose underpinning the collection and use of biometric information increases the likelihood of this information being put to other uses (i.e. function creep), which raises a number of privacy concerns. To alleviate such concerns it is therefore important that the information collected for a biometric application is limited to that information necessary to identify a given individual participating in the application. Many people believe that any additional personal information that may be collected incidentally during the enrolment or comparison phases should be deleted and not held on to in case it might be deemed useful at some time in the future [13],[14]. Of particular concern is the possibility of deriving additional health, medical and sensitive personal information from certain biometric identifiers, the use of which could have far reaching implications for the individuals involved [15];[16].

- **Rights of Access and Redress:** Since privacy, autonomy and bodily (informational) integrity are related to the control and ownership of personal information, it is generally accepted that every individual should be entitled to know what information about them is being stored, why it is being stored, where it is being stored and who has access to it. Article 29 [17]. Privacy and ownership rights are also deemed to entitle a given individual to ensure the accuracy of any information that is stored about him/ her and enable him/her to redress any errors in that [18]. However, under certain circumstances (i.e. in the interest of the common good), for example, where the information is required as part of a criminal investigation, an individual may

be prohibited from accessing, reviewing and/or amending information pertaining to him/her [11]. Notwithstanding such restrictions on accessing the information, the Council takes the view that the information stored about an individual should be kept accurate and up to date. It is therefore important that system operators implement some form of review and correction mechanism. Furthermore, it has been argued that biometric systems and databases should undergo regular audits to ensure that the information is not only correct, but necessary to fulfill the purpose it was collected for [18]. Such auditing may help to alleviate concerns relating to the continued storage of biometric and personal information once an individual has left the biometric programme, for example, if he/she has withdrawn his/her consent to participate, if he/she no longer works for a particular company or attends a particular school that had implemented a biometric programme, or even if the individual has died. Given the expected longevity of many national and international biometrics programmes, the issues surrounding the continued storage and use of information related to an individual who has died are likely to arise in relation to these applications.

Privacy Concerns

The most important issues as regard privacy concerns [19] are briefly discussed below;

- **Creation of large centralized databases:** Data segregation of personal information and biometric information should apply for biometric applications, especially those storing the records of information of many people in a centralized manner. Concerns exist about how this data can be used without the consent of individuals to whom this data is considered private and personal.
- Far-reaching consequences of errors in large-scale networked systems.
- Interoperability that invites unintended additional "secondary" uses.
- **Covert collection:** One concern is the covert collection and use of biometric data, simply because the data is publicly accessible. Facial information, for example, can easily be captured without individuals being aware they are being photographed. Fingerprints can also be easily collected because people leave latent prints when they tough hard surfaces. New iris-based systems can also surreptitiously gather images of people's eyes from a distance of up to two meters. Similarly, palm and finger vein patterns can be captured covertly when people pass their hands over hidden recording devices.
- **Cross Matching:** Concern arises when a biometric trait collected for on purpose is used without a person's knowledge and consent for a different purpose. In biometrics, the potential for multiple uses stems from the fact that some characteristics, such as fingerprints, are relatively permanent and highly distinctive. That makes them a very convenient identifier that is both constant and universal. Once this identifier is collected and stored in a database, it can easily be accessed and matched against future samples, even if they are collected in entirely different contexts. While citizens often favor such cross-matching when police use fingerprints to track down suspects, the same technique can rob innocent people of their right to live in anonymity and freedom from surveillance.
- **Secondary Information:** Another privacy concern relates to the secondary information that may be found in biometric characteristics that were initially collected for a different primary purpose. For example, iris images used in authentication systems can divulge additional information about a person's health, while the wearing down of fingerprints might suggest information about an individual's occupation or socio-economic status. The most powerful example is DNA, which not only identifies a unique individual, but also reveals a wide range of health information.

Protection of Privacy in Biometric System

As stated above, biometrics can have both positive and negative uses. The aim of paper is to not discredit the technology but to create awareness to the risks it purposes as a result of misuse. Biometric data will always be at risk of being misused and abused and the rights of individuals will continue to be violated unless lawmakers start taking into consideration the privacy impact of biometrics technology.

The increasing use of technology and in particular biometric identification systems has not resulted in corresponding legislation and policy [10]. The Universal Declaration of Human Rights includes the right to privacy but the scope of the right's application is vague. The UN Special Rapporteur Report of the Special Rapporteur on the promotion and protection of right to

freedom of opinion and expression, Frank La Rue noted, more entrenched and specific legislation must be adopted to guarantee the recognition of the right to privacy as a human right and to ensure its respect, protection and promotion in all aspects and contexts as well as the need for data protection.

Safeguards must be set down for every step of the process from collection to retention with the right to privacy of individuals at the center. When collecting biometric data, individuals must be informed about the collection procedure, the intended purpose, and the reason why the particular data is requested and who will have access to their data [20].

Individuals must be given the rights to access, correct and delete data saved in their name at any point. The retention period should be justified and guided by the intended purpose in order to prevent the data's use for new, unintended and purposes. [21] Suggested safeguards to minimize abuse and fraud by limiting who has access to it and the form of data which is accessible include using encryption systems or saving only the 'template' (digital data) and not the image itself in the case of fingerprints, DNA and iris [20]..

If biometric data are to be used, centralized mass data systems must be regulated by strict legislation in order to eliminate the possibility of government or third parties (i.e. private sectors actors) taking advantage of the existence of the data for (new) unforeseen purposes. With regards to DNA data, Murphy has put forward several suggestions to safeguard the right to privacy, which could be easily adopted for all forms of biometric data. These include [22]:

- Ensuring that stored data is not subjected to new tests without explicit permission from a court;
- Requesting that a biological sample is destroyed after being used for its intended purpose or once the template is recorded.

Lastly, the development of a biometric constitution, which would establish norms and guidelines to ensure ethical and responsible use of the technology, should be considered [23]. Even if such a document would not be legally binding, its existence would raise awareness and alert policymakers and individuals as to the impact of the use of such technologies on the right to privacy.

Autonomy

Informed Consent

Discussions in the past have emphasized the integral importance of an individual's body to his/her concept of privacy and identity. Integral to these concepts is the notion of ownership of the body and, necessarily, any personal and biometric information derived from or relating to, the body or the person. Question relating to who maintains the control of this information and the access to it, relate not only to an individual's privacy and bodily integrity, but also his/her autonomy. Autonomy signifies an individual's ability to make decisions or take actions based on his/her own principles and free from external influences. In general, an individual's right to autonomy is recognized and respected, provided the decisions of the individual do not result in the harming of others [20]. This view of autonomy is encapsulated and elucidated in John Stuart Mill's "liberty principle", which states that *"the only part of the conduct of any one, for which he is amenable to society, is that which concerns others"*. *"In the part which merely concerns himself, his independence is, of right, absolute"*. *"Over himself, over his body and mind, the individual is sovereign"* (Mill, 1863). An important aspect of autonomy is the idea of informed consent, with the choice of an individual being based on all the details relevant to decision making. In the case, of biometric applications, such details could include what personal information (biometric or otherwise) will be collected as part of the application, the purpose of the collection, how the information will be collected, how and where this information will be stored (e.g. as a template and/or a raw image, encrypted or un-encrypted, etc.), who will have access to the stored information, the duration of storage, whether the individual will be able to see the stored information and amend it or remove if necessary, as well as the benefits and possible risks for participating or not in the biometric programme. In order to make arrangement for informed consent, it is important that the individual understands the purpose and the implications of the proposed system and the potential consequences of his/her own decision to participate or not [18].

Covert Collection of Biometric Information

The rapidly growing advances in surveillance technologies and the potential for remote and distant sensing of certain biometrics, some personal and biometric information could potentially be acquired without an individual's knowledge or express consent. Surveillance cameras for instance collect images and footage of people without their consent for the purposes of crime prevention and investigation. In biometric modalities, currently facial, gait biometrics lend themselves to distance collection;

however, for the majority of biometric identifiers covert collection is not yet fully feasible. While consent to collect biometric information may not be sought, it is generally a requirement to notify people that they could be under surveillance, for example, with a notice proclaiming that CCTV cameras are in operation in that area (Council, 2009). The provision of information in relation to such surveillance programmes can be an important aspect of increasing public awareness and understanding of the programme in operation and its purpose. In addition, providing information to the public may also help to assuage privacy and civil liberties concerns and, ultimately, increase acceptance of such measures (Woodward JD Jr, 2001) in a bid to alleviate concerns regarding the covert collection of surveillance technology.

A company named 3VR in the US has developed an image scrambling algorithm to be used in conjunction with its new facial recognition software. While the facial recognition system is used to identify known suspects (and individuals from watch lists) in the surveillance footage, the image scrambling algorithm is used to blur the faces and bodies of those individuals also in the video footage who are not of interest to the system operators, i.e. innocent people. The blurred images are also encrypted as a further security and privacy protective measure (Scientist, 2009). Nonetheless, despite these developments, some privacy advocates still question the need for CCTV to record surveillance footage constantly, which entails collecting footage of innocent people, as opposed to only recording when something suspect is detected.

The Ability to Opt Out

Consent also implies that an individual should be able to make a voluntary choice regarding his/her participation in a biometric application (Alterman, 2003). There may be situations where an individual does not wish to participate in a biometric application, i.e. he/she opts out. An individual can make his/her decision for a variety of personal, cultural or religious reasons (Woodward JD Jr, 2001). If an individual chooses not to participate in a particular biometric programme he/she should not be disadvantaged or discriminated against and alternative non-biometric means of accessing the same services/entitlements should be provided (Harel, 2009; Wickins, 2007). Moreover, it is considered important not to discriminate against users of non-biometric systems by downgrading or neglecting such systems as a means of encouraging or coercing people to use a related biometric system instead (Harel, 2009). Individuals should not feel under pressure or compelled to enroll in a biometric programme because their work colleagues are willing to do so or because non-participation could result in some level of stigmatization (Commissioner, Annual Report of the Data Protection Commissioner 2007, 2008; Davies, 1994).

Conclusion

Biometric technology is an effective tool for facilitating access to basic social rights but a means of strengthen democracy through establishing legal identities for all individuals, thus facilitating access to rights such as voting and opening banks accounts example of which was the card reader used in election that happen in Nigeria earlier this year and also the bank verification number which was initiated by Central Bank of Nigeria last year. Another example is the initiation of Nigerian Identification Number by National Identity Management Commission, the card which will carry the biometric identity and personal details of each citizen. Biometric technology has proved very useful in the area of security mostly surveillance and profiling of the populations.

However, despite all the positive effects the technology, it still raises concerns for the human rights of citizens like the invasion of privacy, unauthorized use of biometric data without the consent of the individual. There should a law or regulation in place to checkmate people's concerns of privacy invasion. The poor regulation of biometric data means that it is at risk being used for malicious activities or purposes which violates the right of individual by exposing them to profiling, surveillance, and discrimination.

Contribution to Knowledge

This paper has been able to enlighten the public about how privacy can be violated in biometrics without damaging the positive effects of the technology. Biometrics technology has done more good than harm in recent years. The paper is to prioritize the use of the one-to-one identification procedure instead of the one-to-many identification procedure where people's privacy is violated. The paper has been to sensitize people on demand access to ask about their privacy and access to data rights and also asking for their acknowledgement before using their personal information.

Recommendations and Suggestions

The Autonomy highlighted in the body of the paper should be highly considered and implemented. This autonomy are as follows:

- The use of an authentication system over an identification system.
- The ability to opt out of a biometric program.
- Informed Consent of the individual before a stored template is used.
- The purpose of collecting templates should be stated as well as the how the data would be stored and secured.

My suggestion for the readers and researcher is to carry out various researches about ways we can secure biometric technologies without invading privacy.

References

[1] Randall K. Nichols. (1999). ICSA Guide to Cryptography chapter 22. New York: McGraw Hill. International Computer Security Association.

[2] SANS Institute. (2002). Biometrics: A Double Edged Sword-Security and Privacy. SANS Institute.

[3] A.K Jain, R. B. (1999). Biometrics. Personal Identification in Network Society.

[4] Warren S, B. L. (1890). The right to privacy. Harvard Law Review 193, p 29.

[5] Cowen Z. (1969). The Private Man. The Boyer Lectures Australian Broadcasting Commision, 9.

[6] Ethics, B. I. (2005, 04 26). Biometric Information Technology Ethics. Retrieved from Biometrics and Privacy. report of the Second BITE Scientific Meeting: htpp://www.biteproject.org/documents/report_biometrics_privacy.pdf

[7] Lodge, J. (2007). Freedom, security and justice: the thin end of the wedge for biometrics? Annali dell Institute Superiore di Sanitá 43(1), 20-26.

[8] Etzioni, A. (1999). The Limits of Privacy. New York: Basic Books.

[9] Scheeres Julia. (2002). The Positive Side Of Biometrics. Wired News, 20.

[10] Gellman, R. (2013). Privacy and Biometric ID Systems: An Approach Using Fair Information Practices for Developing Countries. CGD Policy Paper, 1.

[11] Council, I. (2009). Biometrics: Enhancing Security or invading Privacy? Irish Council for Bioethics, 63.

[12] Alterman, A. (2003). "A piece of yourself": Ethical issues in biometric identification. Ethics and Information Technology 5(3), 139-150.

[13] Party, A. 2. (2003). Working Document on Biometrics. European Commission, Brussels, 11p. Retrieved from Article 29 Data Protection Working Party (2003). Working Document on Biometrics. European Commission, Brussels, 11p. Available online at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf, accessed 4 April 2016.

[14] Sciences, N. C. (2007). Biometrics, identifying data and human rights. Opinion No. 98. National Consultative Ethics Committee for health and Life Sciences, France, 22.

[15] Mordini, E. (2008). Biometrics, human Body, and Medicine: A Controversial history. In P. Duquenoy, C. george and K. Kimppa (eds.) Ethical, Legal, and Social Issues in Medical Informatics. IgI global, London, 249-272.

[16] Woodward JD Jr, W. K. (2001). Army Biometric Applications. Identifying and Addressing Sociocultural Concerns. RAND, California, 185.

[17] Snijder, M. (2007). Report on the Workshop Security & Privacy in Large Scale Biometric Systems . European Biometrics Forum Dublin, 28.

[18] Commissioner, D. P. (2008). Annual Report of the Data Protection Commissioner 2007. Brunswick Press Ltd, Dublin, 88p.

[19] Canada, O. o. (2011, 11 01). Reports and Publications. Retrieved from Office of the Privacy Commisioner of Canada: https://www.priv.gc.ca/information/pub/gd_bio_201102_e.asp

[20] Bioethics, I. C. (2007). Is It Time For Advance Healthcare Directives? Opinion. Irish Council for Bioethics, Dublin, 98.

[21] Guidelines on the Protection of privacy and Transborder Flows of personal Data. (1980). Organisation for Economic Cooperation and Development (OECD).

[22] Murphy, E. (2013). The Government wants your DNA. Scientific American , 72-77.

[23] Ashbourn, J. (2013). Lack of biometrics standards, loss of personal privacy. Euroscientist webzine.

[24] John Stuart Mill "Utilitarianism" Quotes https://www.brainyquote.com/quotes/john_stuart_mill_201728. Online

[25] Scientist, N. (2009). Encrypted CCTV protects the innocent. New Scientist 2717, 19.

[26] Harel, A. (2009). Biometrics, Identification and Practical Ethics. In E Mordini and M green (eds.) Identity, Security and Democracy: The Wider Social and Ethical Implications of Automated Systems for Human Recognition. . volume 49 NATO Science for Peace and Security Series – E: human and Societal Dynamics, IOS Press, Amsterdam, 69-84.

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

[28] Davies, S. G. (1994). Touching Big Brother: how biometric technology will fuse flesh and machine. . Information Technology & People 7(4), 38-47.

[29] Cavoukian, A. S. (2008). Biometric Encryption: Technology for Strong Authentication, Security and Privacy. International Federation for Infromation Processing Volume 261: Policies and Research in Identity Management, 5.

[30] Crompton, Malcolm. (2002). Biometrics and Privacy. Privacy Law and Policy Reporter 53.

[31] Fred Carter. (2007). Biometric Encryption: Privacy-Enchancing Technology. European Biometrics Forum (EBF), 12.

[32] Management, N. S. (2007). Adoption and Use of Biometric Standards. NSTC, Washington, 11.

[33] David B. and Diane D. (2008). In search of balance: an ethical look at new surveillance and monitoring technologies for security purposes : position statement. Québec (Québec) : Commission de l'éthique de la science et de la technologie, c2008., xxv, 73 p. ISBN 9782550526292.