Review (Narrative)

Ethical Issues in Biometrics

Isaac Cooper, M.S.; Jimmy Yon, M.S.

SUMMARY

In recent years, the social application of biometrics has brought great benefits, but also caused people's concerns about privacy protection, autonomy, and social exclusion. Here we have sorted out the ethical issues related to the application of biometrics, such as privacy protection, functional transformation, body informationization, informed consent, and social exclusion, and analyzed their core and unique issues. We believe that the current management specifications for the development and application of biometric technology are significantly behind their development. In addition to the introduction of policies, the regulation or governance of biometrics technology should also accelerate the practice of ethical governance and regulatory governance.■

KEYWORDS

Biometrics; Ethnicity; Privacy; Autonomy; Social Exclusion

Sci Insigt. 2019; 30(2):63-69. doi:10.15354/si.19.re095.

Author Affiliations: Author affiliations are listed at the end of this article.

Correspondence to: Mr. Isaac Cooper, M.S., Dynamic Biometrics & Cyber Security Co., Chicago, IL 60618, USA. Email: icooper1@dynmetric.com

IN daily life, we often encounter the need to verify identity, or confirm who someone is, which requires identification. The traditional identification methods mainly include two types: one is to identify the identity of the individual through physical objects, such as ID card, smart card, passport, and key, etc.; the second is to identify the relevant password by agreement, such as verification code, password, account number and Password, etc. However, the traditional methods of identification are prone to being stolen, lost, forgotten, etc., which is prone to leakage of personal information, identity theft, fraud, etc., and there are great security risks in identity recognition. Since the "September 11 terrorist attacks", traditional identification methods have become increasingly unable to meet people's requirements for security level growth, and people urgently need more secure and convenient identification methods. Intelligent biometrics is rapidly evolving in this social context (1).

Biometric identification is a method of automatically identifying or confirming a person's identity based on the individual's unique physiological or behavioral characteristics (2). A complete biometric system usually consists of four parts: a reader or a collector, a feature extractor, a database for storing biometric information, and a matcher. Biometric technology has two functions: one is "identification" (who is this person?), which is a "one-to-many" comparison, that is, by comparing the measured template with the centralized database. Multiple templates to identify the identity; the other is "authentication", which is a "1 to 1" comparison, that is, by comparing the specific template in the template and database (both centralized or not) to determine "Is this the person himself declared?" (3).

Any physiological or behavioral characteristics of a person can be used for identification in principle as long as the following conditions are met: (i) universality, the feature exists in all persons; (ii) uniqueness, the feature is unique; (iii) permanent, the feature does not change over time (3). However, in practical applications, the identification system must also consider: (i) performance, the accuracy, speed and resources required to achieve the required accuracy and speed; (ii) acceptability, the degree of acceptance of a particular biometric in everyday life; (iii) deceptive, fraudulent methods to fool the system (4). At present, biometric methods generally accepted include fingerprint recognition, retinal and iris scan recognition, face recognition, hand shape recognition, voice recognition, and signature recognition. Future biometric identification will include DNA analysis, neural wave analysis, and more. Multi-mode systems that integrate different approaches will also be the future of biometrics.

In recent years, with the continuous development of computer technology, the reduction of prices and the improvement of performance, biometrics technology is more practical and social applications are becoming more and more extensive. At present, the technology is mainly used in the fields of work punching, transaction payment, visa, border access control and access control. However, any technological innovation requires constant research on the ethical issues that may arise, and biometrics is no exception (3). It is necessary for us to sort out and discuss the ethical issues arising from the application of biometrics and to explore ways to deal with these ethical issues.

ETHICAL ISSUES IN THE APPLICATION OF BIOMETRICS

Although some problems in the application of biometrics have been studied for a long time from the ethical point of view, there is no holistic and detailed analysis of the ethical issues of biomarkers in the world. Prior to 2007, there were only a few reports on ethical issues in biometrics, such as the 2001 RAND Corporation report "Identification and Addressing Sociocultural Concerns in Army Biometric Applications" (Army Biometric Applications: Identifying and Addressing Sociocultural Concerns) (4), 2003 Working Paper of the Data Protection Working Party of the European Commission (Biometrics) (5), 2004 Biological Vision Report "From User and System Credits" BIOVISION - Roadmap to Successful Deployments from the User and System Integrator Perspective (6), 2004 Economic Cooperation and Development Organization Report "Organisation for Biotechnology" Economic Co-operation and Development (OECD) Report: Biometric-based Technologies (7), 2005 report of the European Commission Joint Research Centre, a forward-looking technology research institute Biometrics at the Frontiers: Assessing the Impact on Society (8), 2006 National Science and Technology Commission's National Biometrics Challenge Report (and other Reports) of the National Science And Technology Council of the United States (9, 10, 11). These reports focus on the following ethical issues: privacy (such as

information privacy, physical privacy, etc.), function creep, indirect medical effects, etc.

Since 2007, several international conferences on ethics, law or policy related to the application of biometric technology have been held with the launch of the RISE project (2009-2012) funded by the European Commission's Seventh Framework Programme (12, 13). The European Biometrics Technology Forum was established in Dublin, Ireland. The academic papers of authoritative journals were published continuously, and the discussion of ethical issues was more in-depth, including some important ethical issues. To sum up, the ethical issues discussed in recent years are as follows:

Privacy

Privacy issues are at the heart of the ethical issues of biometrics (14). Although we have always emphasized the importance of privacy, the understanding of the scope and concept of privacy is different, so it is still difficult to make a clear definition (15). But in general, privacy should include the following two basic characteristics: (i) personal, not others, public or group; (ii) unwilling to let others know, or others cannot interfere. In the 2001 report (4), the US RAND Corporation discussed two privacy issues in the application of biometrics: information privacy and physical privacy. In this report, information privacy refers to the function creep, which means that the use of data exceeds the original purpose, tracking and data misuse. Physical privacy includes stigma, direct damage, and indirect damage. In addition, the Organisation for Economic Co-operation and Development's 2004 report on biometrics (7) focused on security and privacy issues, covering three areas of privacy: functional change, monitoring risk, consent and transparency.

The most in-depth discussion of biometric privacy issues was the 2006 National Science and Technology Council report Privacy and Biometrics (11). The report pointed out that a higher level of privacy should include four areas: decisive, that is, the individual's right to make decisions about things that affect his or her life and body (and sometimes family matters, such as ending life issues); That is, to solve problems related to physical space (such as housing, bedroom, etc.), to decide who can enter or observe activities or objects that occur in a specific space; intentional, that is, to prohibit the retransmission or repeated communication of intimate activities visible to the public; informational, means the problem of using personal information is mainly to control the use of personal information. According to the report, the privacy concept that best fits biometric technology refers to information privacy, and information privacy focuses on a special type of information—personal information. Personal information refers to information used to identify a person. Some data may not appear in the form of personal information, but it can be used to identify a person's identity through joint use. At this time, the data also becomes personal information (11).

Biometric information is collected through observations of individuals and is used to identify individuals such as fingerprints, faces, hand shapes, DNA, etc., which are undoubtedly personal information. However, it is controversial whether the biometric information is stored in the biometric system whether it is still personal information. It is believed that the biometric information stored in the biometric system is not personal information, and is mainly based on the following two arguments: (i) the stored biometric information is meaningless, not personally identifiable; (ii) the biometric image cannot rebuild from the template (14). For the first argument, Roderick B. Woo believed that these stored biometric information numbers are extracted from individuals and are unique and can identify individuals (14) After all, the purpose of collecting this information and turning it into numbers is to identify and/or authenticate a person's identity. Templates (digital or otherwise) are also used to identify individuals. For the second argument, it has been reported in the literature that biometric images can be reconstructed from the template (16, 17). Therefore, there is no doubt that biometric information is stored in a biometric system and still belongs to personal information. Since biometrics are permanent, difficult to change, and generally visible to others, once they are leaked or forged, they cannot be reset, which poses a greater security risk and aggravated privacy issues. Therefore, biometric information should be treated as sensitive data (7).

As a sensitive data, biometric information should focus on its collection, storage and use. The analysis of the 2006 report of the US National Science and Technology Commission focused on how personal information is used, especially whether the use of personal information is appropriate (11). This is also confirmed in the literature, discussion or report of other elsewhere (1, 4, 18, 19). The two most prominent problems here are the function creep and the informatization of the body.

The so-called functional transformation refers to the use of biometric information beyond the original purpose. In 2001, the RAND Corporation's report stated that functional changes may occur in the case of an individual's informed or uninformed circumstances and are inevitable (4). After that, the problem of functional metamorphosis has gradually become a hot topic in the ethical issues of biometrics. Some scholars have suggested that causing functional metamorphosis usually includes three elements: policy vacuum or missing; not satisfied with a given purpose or function; landslide effect or secret application. And through analysis, it is pointed out that the information contained in the biometric system is usually superfluous, and the biometric system cannot avoid redundant information (18).

Informatization of the body is another important issue, but it is also a special type of functional transformation. The term "informatization of the body", originally proposed by Van der Ploeg (20), refers to the ability to extract a large amount of information about individuals from biometric systems. This excavated information is very rich, including some sensitive data, such as medical information, transaction records and so on (11). Biological Vision Report focuses on medical influences. The medical effects of biometrics are divided into two categories (7): direct effects, i.e., damage to the body itself, such as radiation to the body and the spread of disease; indirect Impact, that is, the disclosure of medical information, including the current state of mind and body and potential risk of illness. The report argues that direct medical influence is unreasonable (but some articles argue that direct medical effects are still worrying (21), but indirect medical effects deserve further discussion. The indirect medical influence is to extract medical information from biometric systems. When this medical information (now physical and mental condition and future risk of illness) is leaked to the employer, there is a greater risk (22).

Autonomy

When collecting biometric information, what personal information should I collect (except biometric information, should I include other personal information?), should I inform the collector of the potential risks, how should I tell, whether the recipient should know how the information is stored, what purpose is the information used for, who can get the information, how long is stored, and should the consent of the recipient be obtained again when using the biometric information again? This series of questions is not just about privacy issues, but more about autonomy. An important part of exercising autonomy is informed consent (19). Anton Alterman proposed that biometrics should have informed consent in the application, and individuals who voluntarily submit biometric information should: (i) be fully informed of potential risks; and (ii) be able to understand the possible effects of their actions; (iii) Make such behavior without any threat (23). Therefore, in order to ensure the individual's informed consent, it is important that the individual understands the purpose and meaning of the biometric system (9). In general, adults are considered to have sufficient ability to understand information. The problem is mainly the child's informed consent when using biometrics (24). Similar informed consent issues also come from vulnerable populations such as the elderly, mentally ill, and poorly understood people (9, 25).

Protection of the child's informed consent requires the informed consent of the parent or guardian, but the question is, at what age, the parent or guardian's additional consent is no longer needed. In Ireland, for example, the Data Protection Commission requires that students who are 18 years of age and older make biometrics at school, and students aged 12 to 17 need to obtain the consent of both the student and the parent or guardian, 12 years old. The following students are only required to obtain the consent of their parents or guardians (24). In the case of biometrics in schools in the UK, it is necessary to inform the student and the parent or guardian, but not necessarily with the consent of the parent or guardian (26, 27). It is only necessary to obtain the consent of the parent or guardian if the student is deemed unable to understand the information involved (27).

At present, personal information (including biometric information) is secretly collected without the knowledge of individuals due to advances in surveillance technology and the potential for remote sensing of certain biometric technologies. The most common example is the use of a monitoring probe. The monitoring probe is likely to record the individual's image and whereabouts without the individual's knowledge. While some are for security, crime prevention, and investigation considerations, the Irish Bioethics Committee believes that the secret collection of biometric information needs to be defended under a few preconditions. These conditions include: (i) effectiveness, that is, secret col-

lection of biometric information can achieve social security, prevention / reduction of crime; (ii) proportionality, that is, the degree of monitoring of secret collection of biometric information, measures and personal freedom The degree of restriction is commensurate; (iii) the necessity, that is, the monitoring measures for secretly collecting biometric information is necessary to ensure public safety and achieve national well-being goals; (iv) the least infringement, that is, to secretly collect biometric information for individual rights And minimization of violations of interests; (v) transparency, that is, policies, measures, and actions related to safeguarding social security should be made known to the public (taxpayers); (vi) compensatory, that is, if errors are found in monitoring (good people)) should correct and correct the mistakes in time, and give compensation. The secret collection of biometric information that satisfies the above conditions can be ethically defended; otherwise it will not be defended (19).

Social Exclusion

At present, many biometric technologies are still in the process of development and innovation, and have not yet reached the point where they can be deployed on a large scale. The identification system also needs specific scenarios. In practical applications, there is no guarantee of 100% accuracy, and there is the possibility of Failure to Enroll (FTE), False Non-Match or False Reject (FNM) (28). A study in the UK found that approximately 0.62% of people could not register with any biometric system. The data look small, but multiplied by the total population of the UK made it huge (62,000). At least for now, biometric acquisition devices are not capable of handling individuals other than normal values, and some individuals are not able to be identified and thus excluded. Especially when these systems are linked to social welfare, these unidentifiable individuals are likely to be excluded from social welfare, leading to injustice (25). These groups include: people with disabilities or poor understanding, people with mental illness, the elderly, people of certain races, and homeless people. Wickins believes that in the public interest, at the expense of the interests of the minority, cannot be defended; we should have the same moral responsibility to ensure that these individuals do not incur disproportionate harm (25).

DISCUSSION

It now appears that the application of biometric technology has brought about a series of ethical issues, especially ethical issues related to privacy protection, physical information, autonomy, and social exclusion. The discussion of the above ethical issues abroad mainly stems from the non-government academic conference held in Italy 10 years ago and supported by the European Union - the International Symposium on Bioethics Ethics and Legal Issues. As with other technologies, the ethical issues associated with the application of biometrics are determined by the way it is used, i.e., how the technology is used and how the resulting data/information is handled. When we consider the ethical issues brought about by the application of biometric technology, we should be linked to the innovation and development of other related technologies, such as monitoring technology, big data technology, network information communication technology, database security and other technologies.

Privacy protection is at the core of ethical issues related to biometrics. In the context of biometrics, privacy is more about information privacy and is generally equivalent to biometric information. Unlike general personal information, biometric information has new features such as permanence, invasive concealment, and reveals ability of medical information. Therefore, when collecting, storing, and using/sharing biometric information, it should be treated as sensitive personal information. If not handled properly, there may be many risks such as identity theft and fraudulent biometric systems, and since biometric information is not resettable, these effects will be irreversible. This is what it means to protect biometric information.

Body information is an ethical issue unique to the application of biometrics. If data mining is used properly, it can be applied to the diagnosis and prevention of diseases based on the relationship between certain types of biometrics and certain diseases. However, due to the different values and orientations of individuals, organizations or organizations that use biometrics, body informationization may also lead to risks such as discrimination and stigma, uneasiness and fear, classification and social exclusion.

The discussion of autonomy focused on informed consent. It is undeniable that for national/social/public security, secret or mandatory collection of personal biometric information, exemption or enforcement of indi-

vidual consent does exist, but this cannot be a default state. Such secret or mandatory collection of personal biometric information can only be ethically defended if the conditions of validity, proportionality, necessity, minimum infringement, and transparency are met.

Social exclusion in the context of biometrics refers to the social situation and ethical dilemma that some special groups cannot enjoy because they cannot be recognized by any biometric system. The issue of social exclusion is actually a matter of justice, and personal interests and public interests should be properly weighed. It is reasonable to take certain measures to include as many individuals as possible, and to provide other alternative rights or services for those who cannot be included, and try to avoid social exclusion to harm these vulnerable groups and ensure that they do not incur disproportionate damage.

In addition to the introduction of policies (such as incentives or strong support for technological innovation and maturity, policies established by privacy protection systems), there should be ethical governance and rule governance. . In terms of ethical governance, an ethical framework for evaluating actions in biometrics should be developed. The results of the evaluation include: an action should be done or obligated to do; or this action should not be done or should be prohibited. Or this action is allowed (and not allowed). The ethical framework consists of a set of ethical principles. Each of these principles is an prima facie obligation that we should fulfill, and we must fulfill these obligations if the conditions remain the same. If the conditions change, there is a conflict between the initial obligations, and another initial obligation is more important, then the initial obligation cannot become a practical obligation, and the more important initial obligation becomes the actual obligation. The ethical principles currently discussed are effective, respectful, proportionate, and fair (29), but we still need to explore them further.

Ethical governance plays an extremely important role in limiting and reducing the negative effects of biometrics applications, but there are also shortcomings of insufficient rigidity. Regulatory governance can provide a powerful means to effectively address, control, and address the negative effects of biometrics. At present, although we have a number of laws and regulations on the protection of individual privacy and autonomy, such issues are still worrying and may unconditionally sacrifice the legitimate rights and interests of individuals' privacy and autonomy in various names.

We expect the personal information protection act to be developed as soon as possible, and biometric information should be specifically regulated as personally sensitive information. In recent years, with the innovation of biometric technology, second-generation biometric technology has emerged, including nerve wave analysis, skin gloss analysis, long-distance iris scanning, and advanced face recognition. It should also step up its ethical issues and governance (30).■

ARTICLE INFORMATION

Author Affiliations: Dynamic Biometrics & Cyber Security Co., Chicago, IL 60618, USA (Cooper & Yon)

Author Contributions: Mr. Cooper has full access to all of the data in the study and takes responsibility for the integrity of the data and the accuracy of the data analysis.
Study concept and design: Cooper & Yon.
Acquisition, analysis, or interpretation of data: Cooper & Yon.
Drafting of the manuscript: Yon.
Critical revision of the manuscript for important intellectual content: Cooper & Yon.
Statistical analysis: N/A.
Obtained funding: N/A.
Administrative, technical, or material support: Cooper & Yon.
Study supervision: Cooper.

Conflict of Interest Disclosures: Cooper & Yon declared no competing interests of this manuscript submitted for publication.

Funding/Support: N/A.

Role of the Funder/Sponsor: N/A.

How to Cite This Paper: Cooper I, Yon J. Ethical issues in biometrics. Sci Insigt. 2019; 30(2):63-69.

Digital Object Identifier (DOI): http://dx.doi.org/10.15354/si.19.re095.

Article Submission Information: Received, July 27, 2019; Revised: August 22, 2019; accepted: August 25, 2019.

REFERENCES

1. CSSS Policy Brief No.1. Biometric Identification Technology Ethics. (2003-11-03). https://danishbiometrics.files.wordpress.com/2009/08/news_2.pdf. (2018-4-20).
2. Association for Biometrics (AfB). International Computer Security Association (ICSA). 1998 Glossary of Biometric Terms. Information Security Technical Report, 1998, 3(1): 98-108.
3. Mordini E, Petrini C. Ethical and Social Implications of Biometric Identification Technology. Ann Ist Super Sanita, 2007, 43(1): 5-11.
4. Rand. Army Biometric Applications: Identifying and Addressing Sociocultural Concerns. California: Rand, 2001.
5. EC. Working Paper of the Data Protection Working Party of the European Commission: Biometrics. Brussels: EC, 2003.
6. BIOVISION. Roadmap to Successful Deployments from the User and System Integrator Perspective. Amsterdam: Biovision, 2004.
7. OECD. Biometric-based Technologies. Paris: OECD, 2004.
8. European Commission. Biometrics at the Frontiers: Assessing the Impact on Society. Italy: European Commission Joint Research Centre, 2005.
9. National Science and Technology Council. The National Biometrics Challenge. America: National Science and Technology Council (NSTC), 2006.
10. National Science and Technology Council. Biometrics Foundation Documents. America: National Science and Technology Council (NSTC), 2006.
11. National Science and Technology Council. Privacy & Biometrics. America: National Science and Technology Council (NSTC), 2006.
12. Data Security Council of India. Biometrics and Ethics-EU Project RISE. India: Data Security Council of India (DSCI), 2009.
13. Rebera AP, Bonfanti ME, Venier S. Societal and Ethical Implications of Anti-spoofing Technologies in Biometrics. Sci Eng Ethics, 2014, 20(1): 155-169.
14. Kumar A, Zhang D. Ethics and Policy of Biometrics. Springer-Verlag Berlin Heidelberg, 2010.
15. Thomson J. The Right to Privacy. New York: Cambridge University Press, 1984.
16. Cavoukian A. Fingerprint biometrics: address privacy before deployment. Information and Privacy Commissioner of Ontario, 2008.
17. Feng J, Jain. FM Model Based Fingerprint Reconstruction from Minutiae Template, 2009.
18. Mordini E, Massari S. Body, Biometrics and Identity. Bioethics, 2008, 22(9): 488-498. DOI: 10.1111/biot.2008.22.issue-9.
19. Irish Council for Bioethics. Biometrics, Enhancing Security, or Invading Privacy. Dublin: Irish Council for Bioethics, 2009.
20. Van Der Ploeg I. Genetics, Biometrics and the Informatization of the Body. Ann Ist Super Sanita, 2007, 43(1): 44-50.
21. Tzaphlidou M, Pavlidou FN. Biometrics Applications: Technology, Ethics, and Health Hazards. Special issue. Scientific World Journal, 2011, (11): 529-531.
22. Rachel J, Minter. The Informatization of the Body: What Biometric Technology Could Reveal to Employers about Current and Potential Medical Conditions. In: American Bar Association. Labor & Employment Law Section National Conference on Equal Employment Opportunity Law. Louisiana: International privacy issues panel, 2011: 227–242.
23. Alterman A. “A Piece of Yourself”: Ethical Issues in Biometric Identification. Ethics and Information Technology, 2003, 5(3): 139-150
24. Data Protection Commissioner. Data Protection Guidelines on Research in the Health Sector. Ireland: Data Protection Commissioner, 2007.
25. Wickins J. The Ethics of Biometrics: the Risk of Social Exclusion from the Widespread Use of Electronic Identification. Sci Eng Ethics, 2007, 13(1): 45-54.
26. Information Commissioner’s Offce. The Use of Biometrics in Schools. UK: Information Commissioner’s Offce, 2008.
27. BECTA. Becta Guidance on Biometric Technologies in Schools. UK: BECTA , 2007.
28. Prabhakar S, Pankanti S, Jain A K. Biometric Recognition: Security and Privacy Concerns. Security & Privacy, IEEE, 2003, 99(2): 33-42.
29. European Union. Ethics of Security and Surveillance Technologies. http://grundrechte.ch/2014/opinion_28_securityandsurveillancetechnologies.pdf. (2018–04–20).
30. Mordini E, Tzovaras D. Second Generation Biometrics: The Ethical, Legal and Social Context. Springer Science & Business Media, 2012.■