E

Ethics of Biometrics

Emilio Mordini
University of Haifa, Haifa, Israel
Noria-Onlus, San Vito al Tagliamento, Italy

Synonyms

Biometric ethics; Ethical aspects of biometrics; Ethical implications of biometrics

Definition

Biometrics is a neologism coined by Francis Galton (1822–1911), an English geographer, anthropologist, naturalist, and pioneer in eugenics. Galton modified a previous Greek neologism invented by Anglican priest, and polymath, William Whewell (1794–1866) who first used the term "*biometry*" to mean "*calculation of life expectancy"* (1831). The term was then popularized in 1860s by T.S. Lambert, meaning "*application of mathematics to the study of biology*" (Online Etymology Dictionary 2020). Starting from the 1970s, however, the term has acquired a further and prevalent sense, "*The automated identification or verification of an individual's identity through measurable physical or behavioural traits*" (ISO/IEC 2382-37 2012). In this article we will discuss only this more recent meaning.

According to the EU General Data Protection Regulation "'*biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data*" (The European Parliament and the Council of the European Union 2016).

Engineers usually distinguish between strong, weak, and soft biometric features (Jain et al. 2008). "Strong biometrics" are features that can be considered unique (at least extremely unlikely to be found equal in two individuals) and permanent (at least enduring for long periods of time), they include fingerprints, hand skin patterns, iris structure, hand veins, and the retina texture. "Weak biometrics" are features that are "less unique" or "less stable" than those used as strong biometrics. They include features like body shape, odors, behavior, voice, body sounds, electrophysiological phenomena (e.g., hearth and muscular electrical activity, brain waves, etc.), and gait (analysis of walking patterns); dynamic facial features, eye blinking, lip movements, and smile recognition; voice; signature/handwriting; and so. Finally, with the expression "soft biometrics," engineers refer to features which are too generic to be identifiers. They include categories such as gender, age, race, and ethnicity; weight and height; and eye, skin, and hair color. They can be fruitfully used to reinforce strong and weak biometrics.

S. Jajodia et al. (eds.), *Encyclopedia of Cryptography, Security and Privacy*,
https://doi.org/10.1007/978-3-642-27739-9_1504-1

Background

While biometrics offer certain advantages in many of their applications (e.g., a greater convenience-to-security ratio than traditional authenticators and identifiers such as complex passwords), ethical experts and privacy advocates have argued that these advantages should be carefully weighed against the potential down and dark sides of biometrics (Mordini and Massari 2008).

There are three main categories of ethical concerns surrounding biometric technologies, (1) whether biometrics is inherently demeaning; (2) whether biometrics constitute a building block of the so-called "surveillance apparatus" and a potential weapon in the hands of authoritarian governments; and (3) whether biometrics threaten privacy and data protection.

Human Dignity

The question whether biometrics offend human dignity was raised in the 2000s by prominent, Italian, philosopher Giorgio Agamben, who argued that gathering biometric data is a form of tattooing, akin to the tattooing of Jewish prisoners in Auschwitz. Human life – argues Agamben – is rich of cultural and historical meanings and memories. By stripping people of their names, substituting names with biometric identifiers, rulers deny human cultural heritage, and turn human life into bare life. To Agamben, biometrics risk to be used by rulers to turn citizens into, so to speak, branded beasts. In 2007, the French National Consultative Ethics Committee for Health and Life Sciences expressed a similar concern, "*Do the various biometric data that we have just considered constitute authentic human identification? Or do they contribute on the contrary to instrumentalizing the body and in a way dehumanising it by reducing a person to an assortment of biometric measurements?*" (French National Consultative Ethics Committee on Health and Life Sciences 2007, p. 3).

Surveillance

Biometrics have been also considered integral to the so-called "surveillance society" (Mordini 2014). The word "surveillance" is a French word which literally means oversight, supervision (*surveiller*). During the French Revolution, a network of Surveillance Committees was set up by the National Convention with the task of monitoring all foreigners, listing and arresting suspects, and delivering citizenship certificates. Michel Foucault took this episode to argue that rulers exert their power by controlling citizens' bodies, through a widespread surveillance apparatus (Foucault 1980). Foucault defines the "disciplinary society" a society in which all bodily aspects of life are carefully monitored by authorities. Later scholars have pointed out that Foucault's disciplinary model has been today replaced by a "society of control" where the political problem is no longer monitoring citizens, but rather managing the endless flow of persons, goods, and personal information (Deleuze 1992).

Through biometrics one can identify, trace, and monitor the continuous flow of people which constitutes one of the main elements of globalization. By allowing identification processes on global scale, biometric technologies could even provide a unique and unambiguous identifier to each world inhabitant. This nightmarish scenario – a unique world database, including billions of individuals, run by a global superpower – was evoked by UNESCO, "*If the international system did embrace extensive use of biometrics (. . .), the move could signal the effective end of anonymity. It would become feasible to compile a complete profile of a person's activities (. . .) This death to anonymity would meanwhile be coupled with asymmetry in information: the individual's every move could be monitored, yet he may not have any knowledge of this surveillance. Beyond privacy, such a state of affairs does not bode well for the exercise of other fundamental freedoms such as the right to associate or to seek, receive, and impart information – especially*

as the intimidation of surveillance can serve as a very restrictive force" (UNESCO. Information for All Programme 2007, p. 40).

Privacy and Data Protection

Biometrics have generated several privacy and data protection concerns (Mordini 2008).

Privacy refers to the state of being separated, secluded from others, in contrast to the state of being public or common. According to the *Encyclopedia of Privacy*, it describes and demands "*limits on the appropriation of others' peaceful seclusion, personal information, intimate choice, and identities*" (Allen 2007). In the 1950s, Hannah Arendt was one of the first scholars to observe the political importance of privacy; she reminded us how twentieth-century totalitarian social orders sought to rob people of their privacy in order to better control them. Precisely because of its political functions in the modern context, the private sphere deserves to be protected.

Biometrics can be privacy intrusive at least in two senses: (1) biometrics sensors can be physically or psychologically intrusive, breaking the personal space surrounding individuals and humiliating subjects, and (2) the capture of biometric samples can be conceptualized as an intrusion in the personal informational space, notably when biometrics are captured covertly (e.g., remote facial recognition through CCTV) without informed consent.

The concept of "personal data," which originated in the 1980s, is still related to the notion of privacy but it should not be confused with it. The idea of personal data comes from the increasing capacity of new electronic devises to turn continuous qualities into discrete, measurable, quantities. Personal features and qualities, once described only through narratives and images, can be now expressed in digits, detached from the person and marketed.

Biometric data is considered sensitive personal data, thus deserving a special protection, as data concerning religion, ethnicity, sexual life, etc. (The European Parliament and the Council of the European Union 2016). Biometric data raises concern chiefly as far as biometric databases are concerned, notably (1) centralized databases; (2) dispersed incidental databases; and (3) data linkage and data sharing.

Centralized Databases: The creation of centralized biometric databases, accessible over networks in real time, presents significant security, and data protection concerns. Large centralized databases may increase security risks. If they are compromised, the entire identification system is threatened. They can become important targets for hackers and other malicious entities to exploit. There are also significant risks associated with transmitting biometric data over networks where they may be intercepted, copied, and tampered with, often without any detection (it is to remember that when a biometric identifier is compromised, it is compromised forever). Data protection concerns include: (1) function creep (the expansion of a process or system, where data collected for one specific purpose is subsequently used for another unintended or unauthorized purpose) and insider abuse; (2) lack of proportionality (collected data is disproportionate to the real need); and (3) data misuse, in case biometric databases are used to target and discriminate against ethnical, religious, sexual minorities, persons with disabilities, and so.

Dispersed Incidental Databases: With the expression "dispersed incidental databases," we refer to the huge, random, databases of biometric samples (e.g., faces, body images, body in movement, voices, and so) collected by social media. These databases are more and more often searched, chiefly for forensic and commercial purposes, but they are not ruled by any law or regulation, and are out of subject control.

Data Sharing and Linkage: There are many reasons for sharing biometric data between different actors and agencies; however, when speaking of "biometric data sharing," one usually refers to sharing biometric data between nations for security and law enforcement purposes. Quite often, shared biometric databases consist of a mixed population of data, which includes sentenced criminals, persons only suspected of illegal activities, comprising alleged terrorists

and drug traffickers, immigrants, and so. Data collected for noncriminal purposes, such as immigration-related records, are combined with and being used for criminal or national security purposes with little to no standards, oversight, or transparency. The ethical legitimacy to put all these categories of persons together, to share their biometrics, and eventually to treat them as they were all (potentially) dangerous criminals is highly questionable.

Linkage refers to the creation of multimodal and multibiometric databases, which may embrace several biometrics, including DNA, often linked with other databases, such as credit card, costumer, social insurance, and electronic health record databases. The capacity for eliciting sensitive personal information and profiling of these data networks is huge. Consequently, the risk for function creep and misuse is high. Although some legislations formally prevent data linkage and fusion, other legislations allow them or do not address this issue.

Open Problems

The main open problems are likely to concern next-generation biometrics. Advances in sensor technologies, which enable different bodily and behavioral characteristics to be captured, have been the main technological driver of next-generation biometrics, which is largely based on weak and soft biometrics. We are on the verge of a revolution which is leading us from "biometrics" to "advanced human recognition." Next-generation biometrics progress from asking *who* you are to asking *how* you are; they are less interested in permanent data relating to a pure identity, and more propelled by an individuals' relationship with their environment (Mordini and Tzovaras 2012). What are your intentions and how do you manifest these?

Next-generation biometrics promise to raise questions concerning human dignity, surveillance, privacy, and data protection in a way that first-generation biometrics never quite did, although it is still difficult to predict them accurately. What can be already said is that factors driving biometric innovation must include ethical considerations. In democratic societies, ethics should no longer be conceptualized as a challenge to scientists and engineers but as an opportunity for innovating while respecting fundamental values.

Summary

Biometrics seem to elicit a certain amount of collective concerns. In some quarters, there is a fear that biometric technologies can be potentially "harmful" and this could prove problematic for technology developers and the Governments wanting to employ them. There is thus consensus that ethical, social, and legal dimensions of biometrics need to be adequately addressed. In fact, scientific literature on ethical implications of biometrics is becoming increasingly important. In the period comprised between Jan 2015 and August 2020, the Semantic Scholar corpus indexes 4602 journal articles under the search "biometrics ethics" (Semantic Scholar 2020). In this article, we discuss the main ethical issues raised by biometrics and major trends in this area.

References

Allen A (2007) Privacy, definiton of. In: Staples WG (ed) Encyclopedia of privacy. Greenwood Press, Westport, pp 393–405

Deleuze G (1992) Postscript on the societies of control. October 59:3–7

European Parliament and the Council of the European Union (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Retrieved from Eur-Lex: https://eur-lex.europa.eu/eli/reg/2016/679/oj

Foucault M (1980) The eye of power. In: Gordon C (ed) Power/knowledge: selected interviews and other writings 1972–1977. Pantheon, New York, pp 146–165

French National Consultative Ethics Committee on Health and Life Sciences (2007) Biometrics, identifying data and human rights. Retrieved January 18, 2013, from Comité Consultatif National d'Ethique: http://www.ccne-ethique.fr/opinionsa0a0.html?debut=10

ISO/IEC 2382-37 (2012) Harmonized biometric vocabulary. Retrieved 2020, from International Organization for Standardization: https://standards.iso.org/ittf/PubliclyAvailableStandards/c066693_ISO_IEC_2382-37_2017.zip

Jain AK, Patrick F, Ross AA (2008) The handbook of biometrics. Springer, New York

Mordini E (2008) Nothing to hide. Biometrics, privacy and private sphere. In: Tistarelli M, Juul N, Drygajlo A, Schouten B (eds) BIOID 2008: biometrics and identity management. Springer, Berlin/Heildelberg, pp 247–257

Mordini E (2014) Considering the human implications of new and emerging technologies in the area of human security. Sci Eng Ethics 20:617–638

Mordini E, Massari S (2008) Body, biometrics, and identity. Bioethics 22(9):488–498

Mordini E, Tzovaras D (2012) Second generation biometrics: the ethical and social context. Springer, Berlin

Online Etymology Dictionary (2020) Retrieved 2020, from Biometry: https://www.etymonline.com/search?q=biometry

Semantic Scholar (2020) Biometrics ethics. Retrieved Sept 3, 2020, from Semantic Scholar: https://www.semanticscholar.org/

The European Parliament and the Council of the European Union (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council. Retrieved 2020, from EUR-Lex: https://eur-lex.europa.eu/eli/reg/2016/679/oj

UNESCO. Information for All Programme (2007) Ethical implications of emerging technologies: a survey. UNESCO, Paris