The Use of Biometric Technologies—Normative and Legal Aspects

Limor Ezioni

The development of technology that can identify a variety of physical and emotional characteristics and specifically of biometric technologies has reached a level of maturity and prevalence that require an explicit legal and normative examination of all aspects of their use. The unbridled rush to develop these technologies in Israel and abroad has neglected to address the legal and ethical aspects. This article examines the development of biometric technologies and the ethical and legal aspects of their use. Israel has great interest in the economic development resulting from biometric applications, and this article therefore proposes an international process that aims to create a legal and ethical discussion of the important questions that arise from the broad deployment of biometric technology. In this way, the State of Israel will continue shaping the norms in this field in the future.

Keywords: Biometrics, facial recognition, privacy, databases

Introduction

In December 2018, the British newspaper the *Guardian* published an article about the use of biometric tools in a performance by the singer Taylor Swift, which included hidden cameras for facial recognition in order to compare photographs of the audience with a database composed of photographs of stalkers—compulsive fans of the singer who may pose a security threat for

Dr. Limor Ezioni, Adv., is a criminal law specialist, a senior lecturer at the Academic Center of Law and Science, and a senior researcher in the Cyber Security Program at the Institute for National Security Studies.

the object of their admiration. The security challenges created by stalkers are not to be taken lightly; the singer has a number of known stalkers, against whom restraining orders have been issued, and one has even threatened to rape and murder her. The problem in this context is that the cameras were used without the audience knowing about them or their function.[1]

There were, of course, events that preceded the use of the hidden cameras at Taylor Swift's concert. In April 2019, it was reported that an American youth was suing Apple after being falsely arrested by the company, which employed facial recognition technology in its stores and therefore harmed the privacy of its shoppers.[2] Police arrested the youth in New York after another person had used his pictureless ID and other stolen details to steal from the company's stores in New Jersey, Delaware, and Manhattan. The company used the ID details it had in order to find a picture of the youth, which was then compared with the images produced by the facial recognition technology installed in its stores, leading the company to file a complaint against him with the police. The police then discovered that the youth had been a victim of fraud and was not the real thief.

In the youth's lawsuit against the company, he argued that the connection Apple had made between the stolen items and his true identity, including a photograph of his face that was fed into the stores' security systems, harmed his fundamental rights, without the company having the authority to do so. As a result of the lawsuit, legal experts debated whether the lawsuit had a strong foundation and if, indeed, Apple had contravened the law. Some even claimed that this case realized the vision of George Orwell, with a technology company capable of becoming "Big Brother" and monitoring everyone.

Biometric facial recognition technologies have developed significantly over recent years and are used by security companies in different capacities, which include identifying terrorists in crowded places (train stations, airports, and so forth) by comparing images to existing biometric databases and allowing efficient and controlled entry of crowds to large areas.

This article examines the ethical and legal dilemmas resulting from the employment of biometric technologies in a variety of capacities, by looking at various aspects of the existing legal framework. It is evident already that

1 Laura Snapes, "Taylor Swift Used Facial Recognition Software to Detect Stalkers at LA Concert," *The Guardian*, December 13, 2018.

2 Bob Van Voris, "Apple Face-Recognition Blamed by N.Y. Teen for False Arrest," *Bloomberg*, April 23, 2019.

the development of biometric technologies and biometric databases has reached a stage of maturity and prevalence that require an explicit legal and normative examination of all aspects of their use.

Theoretical Background

The advancement of biometric identification technology has led to a wide range of uses in the private and public spheres. Many workplaces have begun adopting biometric applications as they enable employers to save resources and increase security; however, employees are frequently hesitant to permit the use of biometric data, due to concern that it could be misused.

Darrell Carpenter and colleagues examined three aspects of the use of biometric technologies in the context of privacy. First, they surveyed how the employees of a company that installed biometric systems understood the responsibility of privacy; second, they examined the feeling of vulnerability that biometric systems create; and third, they looked at the notion of the lack of trust in the company. The results indicated that the company was able to diminish the concerns about harming privacy in all three dimensions by including the employees in the drafting of the rules of use for these systems.[3]

Another study examined the use of biometric applications in the healthcare sector, specifically of genome data in the context of cancer and rare diseases, which also has secondary uses that may have been more broadly distributed.[4] The study surveyed the extent to which one can obtain the authority to use private biometric information (in this context, information concerning the mapping of the personal genome) and showed that patients may choose to store genetic information online so that healthcare professionals have access to it. The study addressed the need to ensure that the identity of those who can access the information is properly verified in order to protect patient privacy throughout the process of storing and using the information. According to the study, verification of identity has two functions: preventing impersonation and proving the intent of the use of the information. These are essential steps

3 Darrell Carpenter, Alexander McLeod, Chelsea Hicks, and Michele Maasberg, "Privacy and Biometrics: An Empirical Examination of Employee Concerns," *Information Systems Frontiers* 20, no. 1 (February 2018).

4 Atsushi Kogetsu, Soichi Ogishima, and Kazuto Kato, "Authentication of Patients and Participants in Health Information Exchange and Consent for Medical Research: A Key Step for Privacy Protection, Respect for Autonomy and Trustworthiness," *Frontiers in Genetics* 9 (June 1, 2018).

in ensuring that medical research and exchange of healthcare information are used for appropriate ethical purposes.

Anton Alterman has examined the ethical aspects of biometric identification.[5] He argued that there is both a private and a public interest in biometric identification: they create a balance as there is a kind of tradeoff between the private and the public in using biometric technology for identification purposes. His main conclusion was that the general right to privacy includes the right to control the information that is collected by biometric components and this should be an overriding right. This means that the decision to allow other parties to access personal biometric information must be carefully made, taking into consideration a number of factors, including the accessibility of the information at the expense of losing control over it, information security, and the risks of misuse of the information.

The increasing use of biometric identification makes it necessary for an individual to assess the extent to which he is prepared for his personal information to be sent to other parties in order to receive better and more rapid service. The question addressed is to what extent a person can control the use of his biometric information. Alterman proposes that anyone who is requested to provide biometric information should also be informed of its results and impact in terms of the improved service as a result of rapid biometric identification while at the same time being made aware of the potential risks involved.

In Israel, in 2011, a unit was established in the Prime Minister's Office to develop the field of biometric applications, following the passage of the "Inclusion of Biometric Means of Identification and Biometric Data in Identifying Documents and Databases Law." Later the unit was placed under the responsibility of the National Cyber Directorate.[6] Israel also established a national biometric database, with the goal of preventing impersonation and identity theft. The website for the National Biometric Database Authority states that "in the current situation, and even in a situation of smart biometric documentation but without a biometric database, a person can still impersonate someone else and obtain a number of certificates with different identities

5 Anton Alterman, "'A Piece of Yourself': Ethical Issues in Biometric Identification," *Ethics and Information Technology* 5 (2003): 139–150.

6 The National Cyber Directorate's web page about the Biometric Identification and Applications Unit (in Hebrew) was launched in May 2018. See https://www.gov.il/he/departments/news/bio_aboutbiometric.

simultaneously. This is because in the absence of a biometric database, the Population Authority has no way of ensuring that a person requesting a certificate is not an impersonator."[7] In this context, a distinction must be made between a biometric system that enables identification by cross referencing a person's data with a broad database, which searches for a match within that database (for example, identifying a criminal by a fingerprint, photograph, or DNA) and a system that verifies one's identity by examining a person's biometric details that have been previously sampled (such as passing through the biometric passport line at the airport).

There is a lively debate surrounding all aspects of the use of biometric applications, and even more so regarding the very establishment of the National Biometric Database. Omer Teneh shows the extent to which the Biometric Database Law in Israel could risk harming the right to privacy, should the collection of biometric data not be done for a worthy purpose that is consistent with the values of the State of Israel. According to Teneh, biometric systems create ethical problems as a result of how the information is used. For example, when it is integrated into other system, such as security and tracking cameras, the security purposes of the biometric database could disproportionately harm fundamental values, such as privacy and a person's right to autonomy over his own person. In addition, the development of technology erodes the right to privacy in a permanent and continuous manner, as the technology companies gather a lot of information about internet users through search engines, browsing information, location data, social media connections, and more, enabling identification through irrefutable biometric information. According to Teneh, even though biometric systems may have a positive impact on the right to privacy, enabling identification by using minimal information may also have negative implications on the right to privacy when a person's identity is minimized to "a collection of biometric data."[8]

7 See the National Biometric Database Authority website (in Hebrew) at https://www.gov.il/he/departments/general/target_goals.

8 Omer Teneh, "The Biometric Database Law: Risks and Opportunities," *The Law*, 17, no. 2 (5773–2013) [in Hebrew].

The Biometric Database Authority in Israel has adopted a code of ethics.[9] The code sets forth that the Authority bears practical responsibility for the lawful processing, maintenance, security, and accessibility of the biometric data. The Biometrics Database Authority is also required to maintain the privacy of those whose biometric data it possesses and to prevent any unlawful use. The code of ethics also states that the Authority and its employees must ensure that all activities within the National Biometrics Project are carried out with the goal of serving the public good, ensuring human dignity, and maintaining citizens' rights according to the principles of a democratic society. The code also establishes that the Biometric Database Authority will operate on the basis of minimal biometric data, with it being required for designing ID cards and passports, protecting personal identity, and thwarting the use of counterfeit ID cards and passports.

Israel is not alone in this area as other countries also have established biometric databases. In April 2019, the European Parliament decided to establish a biometric database that could become the largest in the world.[10] The objective is to enable better control over state borders in the European Union. The European biometric database—known as the Common Identity Repository (CIR)—intends to store approximately 350 million identities and will include details such as names, dates of birth, passport numbers, and other identifying details, alongside biometric details, such as fingerprints and facial scans. This data will be available to border authorities and enforcement personnel in EU countries. Even though the European Parliament and the European Council promised "proper protective means" to protect individuals' right to privacy and to regulate enforcement authorities' access to the data, it remains unclear what protective means are being put to practice.

The General Data Protection Regulation (GDPR) of the European Union has posed a challenge for EU authorities in dealing with biometric data. Raul Sanchez-Reillo and others examined the question of how European regulations

9 "The Biometric Database Authority – Code of Ethics," State of Israel, Ministry of the Interior, Biometric Database Authority, 2015. For more information on the ethical aspects of biometric identification, see Annemarie Sprokkereef and Paul De Hert, "Ethical Practice in the Use of Biometric Identifiers within the EU," *Science and Policy* 3 (2007): 177–201; Emilio Mordini and Carlo Petrini, "Ethical and Social Implications of Biometric Identification Technology," *Annali dell'Istituto Superiore di Sanita*, 43 (2017): 5–11.

10 Catalin Cimpanu, "EU Votes to Create Gigantic Biometrics Database," *ZDNet*, April 22, 2019.

could be adopted to protect biometric data.[11] They describe the challenges and recommend a series of measures intended to protect the acquisition and use of biometric information. The process is based on eleven stages, which include determining a level of protection according to the sensitivity of the data; building an isolated work environment in order to minimize the risk of unauthorized access and of direct attacks on the network; using local applications instead of internet-based ones; and deleting or removing of data after its use is completed.

The Development of the Use of Biometric Applications and Their Legal-Ethical Aspects

The use of biometric applications is developing quite rapidly. An article published in the *New York Times* describes the ease with which facial recognition systems can be established in the public space.[12] According to the article, the notion that it is possible to maintain privacy by moving through the public space is mistaken as the facial recognition systems that most cities operate via the existing camera networks threaten that privacy. The article also shows the ease with which people can be monitored without their knowledge. For example, pictures of people in one of the city parks in New York City were collected over a period of nine hours; the pictures were then run through an Amazon facial recognition service, which recognized 2,750 people.

The integration of facial recognition technology with regular CCTV technology, which is installed on street corners, in stores, and in businesses, has enhanced its use and has created a world in which citizens are intensively and permanently monitored.[13] Britain is a leader in implementing this technology; in recent decades, it has installed millions of street cameras. The development of biometric identification systems now makes it possible to use these cameras to identify people and establish monitoring systems at

11 Raul Sanchez-Reillo, Ines Ortega-Fernandez, Wendy Ponce-Hernandez, and Helga C. Quiros-Sandoval, "How to Implement EU Data Protection Regulation for R&D in Biometrics," *Computer Standards & Interfaces* 61 (January 2019): 89–96.

12 Sahil Chinoy, "We Built an 'Unbelievable' (but Legal) Facial Recognition Machine," *New York Times*, April 16, 2019.

13 For more information on the harm to privacy and the mitigation of crime through the use of CCTV cameras, see Andrei Costin, "Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks and Mitigations," *TrustED '16*, Proceedings of the 6th International Workshop on Trustworthy Embedded Devices (New York: ACM, 2016), pp. 45–54.

negligible costs. In practice, these activities have no legal restrictions, with facial recognition technologies being almost unregulated. Moreover, there is no legal framework regulating the use of cameras that rely upon facial recognition technology, nor is there a supervisory mechanism regarding the installation or use of this technology. As a result, the commensurate use of these tools has not been examined, nor is there any balance between the values of freedom and privacy and those of security.

The British use of CCTV cameras has been subjected to increasing criticism, due to the absence of any public discourse regarding the developing technology and the lack of any legal basis for its use. In this context, several important questions have been raised, such as the infringement of citizens' privacy and the degeneration into the "Big Brother" phenomena.[14] A report published in Britain in 2018 argued that the use of this technology constitutes as an unprecedented threat to the privacy and freedom of citizens and may even undermine their basic rights in public places. The report also stated that Metropolitan Police in Britain only had a 2 percent accuracy in its facial recognition system, while the rate of false warnings has reached 98 percent, meaning an innocent person is often wrongly identified as a monitored person.[15]

The United Nations also joined the criticism and published a report that condemned the use of facial recognition applications during a demonstration in South Wales. The report, written by Joseph Cannataci, who was appointed by the UN Human Rights Organization to examine the issue, claimed that the demonstration was peaceful, and the use of the technology was disproportionate to the level of threat to public safety.[16]

Attempts to address this issue in Israel have led to the establishment of the unit of biometric applications within the Prime Minister's Office and later to the legislation of the Biometric Database Law that was approved in March 2017.[17] One of the goals of the law is to attend to the serious problems concerning identification documents, such as passports and ID cards. The law's objective is to establish regulations that would enable the verification

14 Michael Friedewald and Ronald J. Pohoryles, eds., *Privacy and Security in the Digital Age: Privacy in the Age of Super-Technologies* (Routledge, 2016).

15 "Face Off – The Lawless Growth of Facial Recognition in UK Policing," *Big Brother Watch*, May 2018.

16 Chris Burt, "UN Privacy Rapporteur Criticizes Accuracy and Proportionality of Wales Police Use of Facial Recognition," *Biometric*, July 3, 2018.

17 For an in-depth discussion of the advantages and disadvantages of the biometric database, see Karine Nahon, "Private Voice: The Politics of the Biometric Database," in *Law, Society, and Culture* 9, part 2 (2019): 217 [in Hebrew].

of identity and identification of Israeli residents, using biometric means and data. This data would be included in identification documents and stored in the central biometric database, making it difficult to counterfeit the documents, produce double documents for the same person, or use a stolen identity. One of the arguments against the law was that the collection of biometric data does not help to mitigate counterfeiting, and that, at the very most, the data would only be useful for the identity verification of the document holder. It was also argued that it would have been sufficient to create documents that would be difficult to counterfeit.[18]

In terms of using cameras in Israel's public space, the Privacy Protection Authority published a document in 2012 that recognized the problematic nature of expanding the use of closed-circuit systems for a variety of needs.[19] These included crime prevention, traffic direction, and the collection of other visual information. The implementation of the "Violence-Free City" program and the initiative to equip police officers with bodycams led to additional developments on the matter. In 2017, given the technological development and the challenges it posed, the Privacy Protection Authority published a revised draft of the directives in order to receive public comments.[20] Its purpose was to clarify the position of the Registrar of Databases regarding the applicability of the Privacy Protection Law in regards to monitoring cameras in public spaces, particularly when the photographs that they record are stored in databases.

The new draft directive addressed a variety of aspects, including the requirements that cameras in the public space are to be used properly and proportionally and after testing less offensive alternatives; before installing the systems, the scope of their public exposure should be examined and that measures should be taken to minimize it; and cameras and the information recorded by them should only be used for the purpose for which they were installed, on condition that the benefit of using the cameras outweighs the harm to privacy that they cause. The directive also states that the installation of cameras in areas where children are present shall require the explicit agreement of the parents. The directive also restricts the placement and

18 Teneh, "The Biometric Database Law."

19 "Guide Number 4.2012 of the Registrar of Databases – Use of Security and Monitoring Cameras and the Collection of Pictures Recorded By Them," Ministry of Justice, Privacy Protection Authority, October 21, 2012.

20 "The Use of Monitoring Cameras and Databases of the Photographs Recorded by Them," Ministry of Justice, Privacy Protection Authority, September 11, 2017.

number of cameras used, and also requires that cameras be placed only in relevant spaces in order to prevent the photographing and storage of data from spaces that are irrelevant to the stated purpose.

In addition, the Privacy Protection Law allows those who were photographed the right to view the photographs or video recordings that concern them. This law and the Privacy Protection Regulations (Information Security), require that the information recorded and stored by the camera systems be secured. The directive from 2017 relates in detail to aspects of biometric identification and their comparison with databases but explicitly lacks mentioning the restrictions of this technology and its effect on citizens' freedom and privacy.

Engineers and algorithm experts rarely rely on social research, nor the other way around. Thus, biometric applications are considered a mysterious "black box" that contain unique information about people and conduct, as well as comparative and matching identity verification processes. The combination of mathematical calculations and biological data apparently provides technical and scientific-objective legitimization to the field of biometric applications. In this context, we must remember that biometric technologies are increasingly involved in automatic decision-making, without human intervention. As a result, the ethical dilemma increases regarding social screening, which could lead to discrimination based on external biological characteristics.

Conclusion

The development of biometric technologies to identify a variety of physical and emotional characteristics has reached a level of maturity and prevalence, which require explicit legal and normative examination of its use. The non-stop rush to develop these technologies in Israel and abroad has neglected these aspects. Israel has a high level of interest in the economic development of biometric applications, and therefore it would be wise for the relevant authorities (the Ministry of Justice, the Privacy Protection Authority) to lead an international process of developing an ethical and legal discussion on the important questions that are raised by the distribution of this technology, particularly biometric technology. In this way, the State of Israel will be able to continue to shape this field in the future.

In the past, biometric technology was restricted to security and enforcement needs. However, the current situation is different. Biometric applications are

increasingly prevalent in both the civilian and commercial sectors. The broad distribution of biometric applications makes it extremely important to address the ethical problems inherent in the development and use of this technology. We are obligated to research and develop knowledge regarding the ethical and legal implications of its use for civilian and commercial organizations, and the question of privacy is a key issue that must be examined. Despite the spread of biometric technology, there is very little empirical research on applicative biometrics and ethics in the civilian and commercial sectors. The development of knowledge therefore requires examining the potential damage that could be caused by biometric monitoring.

The field of biometrics should not be seen only as a technological development; rather, we must deepen our understanding of its legal and ethical implications in order to formulate a sophisticated legal and regulatory framework that can better deal with the different challenges expected in this field in the future.