Facial Recognition in Israel's Public Places Policy Principles & a Call for Regulation

The Identity and Biometric Applications Unit

The Israel National Cyber Directorate (INCD)

July 2021

Contents

Introduction 3

The technological development of facial recognition 4

Facial Recognition in Public Places 6

A call for regulation 9

The Risks In Using Facial Recognition in Public Places 9

Regulating the Use of Facial Recognition in Public Places Around the World 10

Policy Principles – The Use of Facial Recognition in Israel's Public Places 14

Conclusion 18

Acknowledgements 19

Technology Appendix 20

Deployment of a Facial Recognition System in Public Places (Cyber Considerations) 20

Proper Management of Biometric Systems (Biometric Considerations) 21

Introduction

1. The Identity and Biometric Applications Unit (INCD) has formulated a National Policy and Guidelines for Biometric Applications, in accordance with Government Decision 4510, from 1.4.12. The policy refers to technology, privacy, security, and ethics perspectives pertaining to government activities, in public and private sectors [1].The policy paper deals with general biometric applications and does not focus on any particular biometric technology or application.
2. Facial recognition in public places is a biometric application that utilizes photo capture and facial recognition capabilities of non-cooperative subjects in public places, and then compares the faces captured with those stored in a dedicated database. With recent years' dramatic improvement in facial recognition technology's precision, the use of cameras in public places, sensitivity surrounding the subject and its special technological perspectives, as well as future-forward thinking in light of global biometric systems usage trends, it was decided to formulate policy principles for this specific application, and to call for regulation, accordingly
3. Initially, our analysis was presented at a Parliament (Knesset) Science and Technology Committee session on 15.12.2020, prior to which a report by the Knesset's research center was published[2]. As mentioned in this report, as well as during the Knesset session, there are no all-encompassing policies or regulations in Israel, nor are there any specific legislations that standardize the use of advanced monitoring technologies, such as those used for facial recognition.
4. **We conclude that action must be taken to regulate this sensitive subject in primary legislation, while holding public discussions in larger forums to properly weigh risks against benefits, and place emphasis on ethical and other considerations involved.** There is extreme importance in regulating "the rules of the game," so as to, on the one hand, enable law enforcement (or other controllers) to fulfill their roles and tasks by leveraging technology and, on the other hand, clearly define the bounds within which said controllers must act, to avoid undue harm being caused to Israel's citizens and society, as a whole.
5. **The goal of this document is to present all of the issues that should be examined within this framework.** As such, this document includes selected examples of regulations from the Western world, with standout cases, such as the EU's proposal for AI regulation that

[1] National integrative policies for biometric applications
https://www.gov.il/he/departments/news/bio_biopolicy_app
[2] Knesset committee report on the use of recognition technology and monitoring in public spaces
https://fs.knesset.gov.il/globaldocs/MMM/2503c32b-2f94-ea11-8104-00155d0aee38/2_2503c32b-2f94-ea11-8104-00155d0aee38_11_16517.pdf

specifically refers to the use of enforcement solutions, when using biometric systems for the remote identification of people[3]. Additionally, a comprehensive survey of various perspectives pertaining to regulating the use of these systems, compiled by Tel Aviv University's Yuval Ne'eman Institute, has been attached[4].

6. This document does not present a comprehensive, principled discussion on the legitimacy of the goals for operating image capturing systems in public places, a subject that increases in its sensitivity when relating to facial recognition systems. We believe that a comprehensive discussion should be held in a broader forum.
7. Additionally, it must be made clear that this document does not address the National Smart Documentation project that integrates biometrics and includes facial recognition (in accordance with dedicated legislation[5]). Additionally, it does not touch upon the use of facial recognition in other systems that require user participation (such as access control systems), nor does it pertain to facial recognition in the virtual world (such as on social networks).
8. Relevant government background documents include a compilation of recommendations published by the INCD on the subject of reducing cyber risks pertaining to security cameras[6] (April 2018); documents released by the Israel Privacy Protection Authority[7]; and the National Policy and Guidelines for Biometric Applications. The current document details additional technology perspectives that are relevant to these systems (particularly biometric perspectives).

The Technological Development of Facial Recognition

9. Facial recognition system is a computer application that includes an algorithm capable of automatically or semi-automatically identifying or verifying a person's identity, based on digital photographs or video frames. One of the ways this is done is by comparing specific images to those images stored in a database (referred to as 1:Few or 1:Many), or by comparing a specific captured image to a specific stored image (known professionally as 1:1).

[3] https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF

[4] Available in Hebrew at our website: https://www.gov.il/he/departments/general/face_recognition

[5] The Israeli Biometric Applications Commissioner (who leads the National Cyber Directorate's Identification and Biometric Applications Unit) supervises the National Smart Documentation project, and advises on policy regarding that project, in accordance with the Law on biometric identification mechanisms and data inclusion in the e-documents and Central Database from 2009.

[6] https://www.gov.il/he/departments/policies/iotcamers

[7] https://www.gov.il/BlobFolder/policy/surveillance_cameras_guidelines/he/The%20use%20of%20security%20cameras.pdf ; https://www.gov.il/BlobFolder/reports/drone_recommendations/he/PPA_DRONE_RECOMMENDATIONS.pdf

10. Facial recognition systems are currently used for a variety of civilian and commercial purposes, from verification and identification in the financial sector (opening bank accounts, accessing digital services, etc.) access control at places of work, patient identification by healthcare systems, and customer identification at various businesses, to identification and verification on social networks, at international border crossings, and to produce national/official documentation. These systems are also used for various security purposes, such as law enforcement, maintaining public safety/order, and counter-terrorism activities.
11. Up until a few years ago, facial recognition algorithms geometrically compared facial features and the differences between them: eyes, nose, mouth, ears, etc. In addition, certain algorithms studied additional factors pertaining to facial structure, such as facial skin texture. In recent years, we have witnessed changes in the types of algorithms at the foundation of facial recognition technology; more and more technologies now rely on Deep Convolutional Neural Network algorithms, which are based on neural networks and machine learning (a subdivision of a field called artificial intelligence). This approach was inspired by cognitive processes that take place in natural neural networks, such as in the human brain. Each of the network's processors executes a simple mathematical equation. By integrating all of the equations, the network's processors are able to engage in complex behavior.
12. The change in facial recognition algorithm's operations has enabled a significant upgrade to their performance capabilities. Namely, a significant decrease in error rates when comparing images (100 times better over the past decade), especially when referring to controlled images (images captured in cooperation with their subject, in a controlled environment and in accordance with ICAO specifications[8].
13. Advancements in the development of facial recognition technology has, in recent years, led to a significant increase in the use of these systems in a variety of situations. Namely, an increase in their use has influenced a rise in commercial entities' desire to invest – money and effort – into this field[9], creating new technological challenges that mostly pertain to the

[8] Face Recognition: Performance, Measurement; Patrick Grother and Mei Ngan; NIST; Biometrics Institute Workshop Sydney, AU; May 29,
See additional information in the statement released by the Israeli Biometric Applications Commissioner, in accordance with Clause 2B of the Law on biometric identification mechanisms and data, stipulated in the 2009 Identification and Database Documents, from 27.5.2020.
https://fs.knesset.gov.il/23/Committees/23_cs_bg_584569.pdf
The ICAO standard is an international aviation standard that establishes the manner in which images can be captured for passports/national identification documents.

[9] Examples of several spaces within which significant resources are invested into facial recognition technologies: smartphones, social networks, and Fintech.

need to cope with fraud, also referred to as presentation attacks, or PA[10], as well as with other malicious activity, such as deep fakes[11]. We believe that the improvement described above will continue to trend positively and grow.

14. Alongside the significant improvement in facial recognition technology capabilities, there are other factors that influenced the increase in technology usage, such as the relative ease with which facial images can be captured, allowing for the optimal use of biometric applications, with the ability to compare images with high levels of precision, and the ability to store and retrieve many facial images within the virtual space, which enables the creation of databases that can be used for facial recognition comparison..
15. These developments led to a significant increase in the facial recognition technology market's valuation: global revenues were estimated at 3-5 billion dollars between 2016-2019 and are expected to double between 2022-2026 to 7-10 billion dollars[12].
16. There are several Israeli national projects that utilize facial recognition in a highly-controlled manner. Standout examples include the Smart National Documentation project (The Population and Immigration Authority and The National Biometric Database Authority), the Police Department's biometric databases (suspects, defendants, and criminals), and the Biometric Program for Foreigners (The Population and Immigration Authority)[13].
17. Facial recognition is integrated within automatic gates at the airport (verification/comparison with passport images), in banking systems for the purpose of opening new bank accounts online and under certain conditions (within the framework of the Electronic Know Your Customer principles), by Israeli social media users (i.e. Facebook), to open cellphones, and others.

Facial Recognition in Public Places

18. Facial recognition in public places is a specific biometric application, for which images of people are captured in public and compared against biometric images stored in a database, without the subjects' cooperation). Performing **facial recognition on people in a crowd without their cooperation with the identification process** is harder to execute than

[10] Presentation of false representations to the system, so as to disrupt the biometric process. With respect to facial recognition systems, such an attack can involve the presentation of a print image, an image of someone wearing a mask, etc.

[11] Synthesis of falsified facial images of video clips via artificial intelligence-based computer processing.

[12] United States Government Accountability Office, "Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses", July 2020 - https://www.gao.gov/products/gao-20-522

[13] See details in the Knesset's Research & Information Center's report, Footnote 2. These projects are regulated by primary legislation, except for the Biometric Project for Foreigners, for which a legislative memorandum was published. A Knesset debate has yet to be held on the matter.

conducting facial recognition processes in a controlled setting. Accuracy rates with respect to facial recognition in public places are lower, as these systems must cope with people moving about, hidden features, different angles, changing environmental conditions (weather, lighting, and more), which can lead to different and low-quality facial images ("Faces in the Wild").[14]

19. When activating facial recognition applications in public places, passersby are photographed, and these images are either temporarily or permanently stored, and compared to images included in a "watchlist"[15] or some other database. There may be cases in which images are captured in a public space but are not immediately (in real-time) subject to biometric comparison; these images are collected to enable biometric comparison at a later date, in hindsight.
20. Facial recognition is used in public places in several scenarios, worldwide, such as in airports for "traveler management[16]," at sports fields and other large-scale sporting events[17], at protests[18], etc. It is also used by security and law enforcement officials around the world[19], as well as by local authorities ("smart cities")[20], and can also be used for various commercial purposes, such as to identify customers frequenting places of business, and offer them products or discounts[21].
21. With respect to the Covid-19 pandemic, there are news reports indicating that the Russian government has used broad facial recognition capabilities that include using "watch lists[22]"

[14] A 2017 American National Standards Institute (NIST) report that presents the challenges attributed for facial recognition when dealing with a non-cooperative audience and video capture for surveillance purposes - https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8173.pdf

[15] In security situations, a watch list is a list of people of interest – suspects, terrorists, etc., who are wanted by law enforcement officials.

[16] Identification of airport travelers from the moment they arrive at the airport and until their flights take off, at relevant stations. In this case, the use of facial recognition is for security and service purposes.

[17] For example, spreading our facial recognition systems at the 2020 Olympic Games in Tokyo: https://www.theverge.com/2018/8/7/17659746/tokyo-2020-olympic-games-face-recognition-nec

[18] See the attempts made by protestors to disrupt facial recognition use by law enforcement officers at demonstrations in Hong Kong: https://www.diyphotography.net/hong-kong-protesters-are-using-laser-pointers-to-confuse-facial-recognition-and-theyre-frying-photographers-camera-sensors/

[19] Facial recognition cameras are currently massively being used by the Chinese government. See, for example, the BBC's report on over 170 million cameras installed within China's public spaces: https://www.bbc.com/news/world-asia-china-43751276;
An article describing the German police's increased use of facial recognition systems for 1:1 comparisons: https://digit.site36.net/2021/01/20/facial-recognition-at-german-police-authorities-increased-by-more-than-a-third/
British law enforcement's use, described below. See content on the Wales Police website as well: https://afr.south-wales.police.uk/

[20] https://www.smartcitiesworld.net/news/outdoor-surveillance-cameras-to-be-biggest-iot-5g-sector-until-2023--4712 ;
https://www.planetbiometrics.com/article-details/i/8636/

[21] https://www.youtube.com/watch?v=PZKgAuk6kLM ;
https://www.youtube.com/watch?v=bpfvloDVIe0

[22] https://www.bbc.com/news/av/world-europe-52157131

to identify quarantine violators in the public space. There are similar reports about China as well (with the added temperature gauging capability)[23].

22. It is our impression that, current use of facial recognition capabilities in public places[24] in Israel is less significant than what is implemented abroad, including in Western countries. With respect to law enforcement purposes, several petitions have been filed pertaining to the use of facial recognition applications in public places[25], and there are reports about applications that have been used in sports stadiums[26].

23. Additionally, image capturing is activated in Israeli public places by local authorities[27] and private companies[28], without directly activating facial recognition application, for security and other reasons[29]. The images captured can be scanned for facial recognition purposes, at a later date. Also, there are some reports about the use of facial recognition capabilities within Israel's public space, for commercial purposes[30].Generally speaking, the use of facial recognition by Israeli law enforcement officials (the police, in particular) or local authorities is limited. One can assume that the use of this technology will increase in line with global

---

[23] https://www.dw.com/en/using-facial-recognition-against-covid-19/av-53868752;
https://www.scmp.com/abacus/tech/article/3104512/facial-recognition-data-leaks-rampant-across-china-covid-19-pushes;

[24] A report published by the Knesset's Research and Information Center on the use of technology for identification and monitoring purposes in public spaces (Chapter 2) -
https://fs.knesset.gov.il/globaldocs/MMM/2503c32b-2f94-ea11-8104-00155d0aee38/2_2503c32b-2f94-ea11-8104-00155d0aee38_11_16517.pdf

[25] Recently, freedom of information petitions were filed with respect to the police and the IDF's use of facial recognition applications in public spaces (see Petition 27229-09-20 The Association for Civil Rights in Israel v. the Israeli Police Department; Petition 46723-09-02 The Association for Civil Rights in Israel v. The Supervisor of the Freedom of Information Law in the IDF (to complete the picture, it's important to indicate that a petition was filed on the "Ein Netz" police system that identifies car license plates); Petition to the High Court 641/21 The Association for Civil Rights in Israel v. The Israeli Police Department.
https://01368b10-57e4-4138-acc3-01373134d221.usrfiles.com/ugd/01368b_0cb9878b629f405a8368cea5e9493927.pdf

[26] Facial recognition cameras at the Sami Ofer Stadium (2014) - https://www.one.co.il/article/235161.html
Facial recognition cameras at Netanya Stadium -
https://www.netanya.muni.il/?CategoryID=2524&ArticleID=5698
Facial recognition cameras at Teddy Stadium (2017) -
https://www.globes.co.il/news/article.aspx?did=1001197890

[27] The "City without Violence" program – The Ministry of Labor, Social Affairs, and Social Services -
https://www.gov.il/he/Departments/General/molsa-community-innterventions-city-without-violence;
Article in Haaretz on cameras in Tel Aviv-Jaffa -
https://www.haaretz.co.il/news/education/.premium-MAGAZINE-1.8445403;
A report published by the Knesset's Research and Information Center on the use of technology for identification and monitoring purposes in public spaces (Chapter 3) -
https://fs.knesset.gov.il/globaldocs/MMM/2503c32b-2f94-ea11-8104-00155d0aee38/2_2503c32b-2f94-ea11-8104-00155d0aee38_11_16517.pdf

[28] The use of facial recognition to unlock WIND's shared e-scooters -
https://www.themarker.com/technation/.premium-1.9233134

[29] Article on Channel 12 - https://www.mako.co.il/news-channel2/Channel-2-Newscast-q3_2019/Article-3b43a949840bc61027.htm?Partner=searchResults;
Company website - http://wise-sight.com/ ;

[30] The Victory grocery chain piloted the use of cameras that monitor customers' emotional responses to in-store products - https://m.calcalist.co.il/Article.aspx?guid=3846114

trends, especially in light of the Covid-19 pandemic, the desire to avoid physical contact, and the need for remote identification processes.

24. **With respect to the Covid-19 pandemic**, attempts were made to use photo capture in Israeli public places to locate and alert on unmasked people, with[31] or without deploying facial recognition[32].

A Call for Regulation

The Risks in Using Facial Recognition in Public Places

The following will outline the main risks involved in using facial recognition in public places (these risks also exist when using controlled systems, albeit to a lesser degree).

25. Errors leading the harassment of innocent people – managing a biometric applications system is a complex task, as many environmental and external sources are likely to influence its performance. The system's failure to perform as intended can lead to errors in identification and the harassment of innocent people (FPIR); it can also lead to a failure to identify suspects (FNIR)[33].

These failures can transpire for several reasons, including as the result of establishing too-low of a threshold for matches to be made; untrained analyses of the system's results; insufficient integration of the system's elements or improper selection of elements from the start; incorrect camera placement; special audience characteristics that were not taken into account; algorithm's demographic biases; and others. Namely, it is not enough to establish "administrative" limits and implement them to a degree; there is a real need for facial recognition systems to undergo precise **technological deployment**, as the application has been proven to fail, in instances where the technological deployment was incorrect[34].

It is needless to say that the incorrect identification of innocent people can lead to severe infringements on their rights, depending on the system's intended purpose[35].

---

[31] A pilot that tested out the use of a facial recognition and temperature measuring system at the entrance to Bnei Zion Hospital - https://www.ynet.co.il/articles/0,7340,L-5716252,00.html

[32] In May of 2020, several hospitals, including Sheba Tel Hashomer, installed systems to identify mask wearing - https://www.globes.co.il/news/article.aspx?did=1001328104; https://www.israelhayom.co.il/article/760909

[33] FPIR- False Positive Identification Rate; FNIR- False Negative Identification Rate

[34] A BBC article that describes facial recognition systems used in Britain's public space, which exhibit a 90% false alarm rate - https://www.bbc.com/news/technology-44089161

[35] For example, the New Jersey Police Department arrested and imprisoned an innocent man for 10 years, due to a facial recognition system's identification failure - https://futurism.com/lawsuit-claims-facial-recognition-ai-sent-wrong-man-jail;
An article on "60 Minutes" about a facial recognition system's error that led to an innocent man's arrest - https://www.cbsnews.com/news/facial-recognition-60-minutes-2021-05-16/
Another case of a reported misidentification -

26. Monitoring, infringements on privacy, and a "sense of being watched" –facial recognition in public places is currently used worldwide to "maintain public order" at sports stadiums, performances, protests, "at-risk" areas, etc., worldwide. Additionally, facial recognition mechanisms are likely to be used for commercial means within public places, such as identifying and targeting VIP customers with promotional content and/or special offers. This practice is likely to lead to over-hoarding of many people's facial images, having culled them from different locations in a manner that can lead to said people being monitored, and their movements, political beliefs (participating in a protest, for example), and consumer behaviors documented, influencing how the general population is kept in check and policed. As such, this form of monitoring can create a "chilling effect" that infringes upon singular persons' sense of privacy, freedom, and freedom of expression, ultimately harms the individual. Furthermore, there is cause for concern that biometric information can also be used for purposes that were not established or made clear from the start ("function creep").
27. Information leakage and its use by unauthorized people – The leakage of biometric information from databases used for facial recognition in public places can lead to the contents and capabilities of said databases' malicious use and by unauthorized sources, without effective supervision and control. Should this risk become reality, it would lead to the privacy infringements detailed above and/or cause harm to other interests, including security interests (for example, by collecting intelligence, monitoring targets, etc.) and cyberbullying (via Deep fakes, for example)
28. Increased use of facial recognition technology, the potential for using biometric applications via simple photography without the subject's knowledge, and the storing of facial images in large and relatively accessible databases – significantly increase the risks detailed above.

Regulating the Use of Facial Recognition in Public Places around the World

29. Concerns rising from the use of facial recognition in public places: there has recently been much public discourse on the subject in the Western world – in Parliament debates, news publications, non-governmental organizations' papers and even within the industry itself.

The following are **several examples of legislative processes dealing with facial recognition in public places around the world** (further detailing appears in a more comprehensive report published by Tel Aviv University's Yuval Ne'eman Institute[36]):

https://www.law.com/njlawjournal/2021/01/15/rise-of-the-machines-facial-recognition-technology-heralds-upswing-in-litigation/?slreturn=20210109042210

[36] see footnote 4

30. In the United States, several legislations were proposed at local, state, and federal levels, with respect to the field of facial recognition in general, as well as regarding facial recognition in public places in particular.
The state of Illinois was the first state in the US to deal with regulating the biometric field as a whole with its 2008 legislation. However, this legislation does not specifically relate to facial recognition in public places[37].
One decade later, in May of 2019, a proposed law was passed in San Francisco, according to which facial recognition technologies cannot be used in public places by municipal entities[38]. In September of 2020, the city of Portland adopted the country's most rigorous laws pertaining to facial recognition[39], which banned any and all private or governmental use of facial recognition technology.

Washington State is home to vast legislative activities designed to regulate the use of facial recognition mechanisms, including those operating in public places. As of 2019, nine (!) proposed laws were filed on the matter. Today, there are three laws pertaining to the collection of biometric information of facial recognition in public places in Washington State, two of which ([40]HB.1717 and [41]SB.6280) apply to local and state government entities alike and one ([42]HB.1493) applies to the private sector.

Law SB 6280 ("An act relating to the use of facial recognition services") refers to the activation of facial recognition applications by government agencies, and places particular focus on facial recognition in public places. Among its stipulations, it establishes that no use is to be made of facial recognition applications for ongoing monitoring, unless severe crimes are involved and a judicial warrant is produced (in emergent cases, one can act so long as approval is received from the agency's head, and a warrant is produced within 48 hours). In addition, the law requires meticulous management of said systems, and attention to be paid to its error rates, possible biases attributed to its algorithm, adopted security measures, third-party system inspections, and impact surveys on rights infringements (and more), as well as mandatory submission of public reports detailing the activated systems. Furthermore, the law stipulates that the judiciary authority will monitor the decrees allowing the use of facial recognition and rejected requests.

---

[37] The Illinois Biometric Information Privacy Act ("BIPA")

[38] https://www.wired.com/story/san-francisco-could-be-first-ban-facial-recognition-tech/

[39] https://spectrum.ieee.org/tech-talk/artificial-intelligence/machine-learning/facial-recognition-and-the-us-capitol-insurrection

[40] https://app.leg.wa.gov/billsummary?BillNumber=1717&Year=2017

[41] https://app.leg.wa.gov/billsummary?BillNumber=6280&Year=2019&Initiative=false

[42] https://app.leg.wa.gov/billsummary?BillNumber=1493&Year=2021&Initiative=false

The law further establishes that a "task force" comprised of various representatives (from the government, academia, industry, third-sector, etc.) will be established and charged with publishing recommendations vis-à-vis coping with threats related to the use of facial recognition technology; examining the effectiveness of existing state legislations on the subject; and examining the quality, accuracy, and effectiveness of facial recognition services.
Over the past two years, bills on facial recognition were proposed and approved in others states, and proposed legislation made its way to the American Senate, but have yet to be approved[43].

31. At this time, Britain lacks dedicated legislation for facial recognition in public places. However, the subject has been raised in parliamentary discussions and reports, and has been referred to by several important figures, including (and led by) the country's Biometrics and Surveillance Cameras Commissioner[44].
The main context, within which this subject is discussed in Britain, is its use in public places by law enforcement officials. This subject was deliberated in local courts in a case where the Welsh police activated facial recognition in public on several occasions [45]. The Court of Appeals found some of the petitioner's claims justified, and it was established that the existing judicial framework in Britain lacks an appropriate response to two important questions: which people are included in "watch lists" and where can facial recognition systems be deployed in public places. The court added that, in such a case, police officers in the field have too much discretion, and that their weighing of risks against civil rights with respect to the use of facial recognition systems is lacking. It is important to indicate that the court did not overwhelmingly ban the activation of said technology, but rather emphasized the importance of its measured activation, in accordance with particular limitations.

---

[43] The Facial Recognition and Biometric Technology Moratorium Act- https://www.markey.senate.gov/imo/media/doc/acial%20Recognition%20and%20Biometric%20Technology%20Moratorium%20Act.pdf ;
Ethical Use of Facial Recognition Act- https://www.congress.gov/bill/116th-congress/senate-bill/3284/text

[44] Until 2021, there were separate regulators for biometrics and surveillance cameras in Britain, however these roles have since been unified. Reports from the relevant professionals were published on the subject of facial recognition in public spaces:
In November of 2020, the Surveillance Cameras Commissioner published guidelines and their recommended approach to the use of police surveillance cameras that include facial recognition systems, in public spaces[44], for the purpose of locating suspects on watch lists - https://www.gov.uk/government/publications/police-use-of-automated-facial-recognition-technology-with-surveillance-camera-systems
The Commissioner believes that access should be granted to "live" facial recognition usage (LFR) for police work, but that said access should be controlled by legislation. Additionally, the Commissioner said that the Parliament should decide whether to allow the use of '"live" facial recognition technologies by police forces, and for which purposes.
https://www.gov.uk/government/news/biometrics-commissioner-on-the-police-use-of-live-facial-recognition

[45] https://www.judiciary.uk/judgments/r-bridges-v-cc-south-wales/

32. Early in 2020, the European Union announced that it was considering banning the use of facial recognition in public places for a period of five years. However, it later retracted the statement, emphasizing the need for clear criteria pertaining to the subject[46].
In April of 2021, the first legislative framework[47] referring to risks related to AI use, including for facial recognition in public places (RBI Systems- Remote Biometric Identification systems), as well as to the EU's role, with respect to this subject. This proposal was meant to ensure that the use of AI systems in the EU is safe, transparent, ethical, unbiased, and supervised by humans.

According to this proposed regulation, law enforcement officials cannot make use of biometric systems for "real-time," remote identification purposes, in public places, except for in extenuating and necessary cases, and for particular purposes: focused searches for crime victims (such as missing minors); coping with emergency situations related to public security and counter-terrorism activities; or locating and identifying accused criminals for the purpose of bringing them to justice for severe crimes[48].

In these very extreme situations, the circumstances surrounding the event should still be taken into consideration, as should the potential for damage, and other possible implications on individual rights. In addition, these unique cases will be regulated, so as to limit the duration, geographic region, and data arrays made use of by the system.

Moreover, the proposed regulation establishes that remote biometric systems (RBI) that are activated in "real-time" or "near-real time" (post) to identify people involve high levels of risk. As such, they must be examined by a third-party (court of law or independent authority), before approval can be granted and the system can be deployed. The court or authority will only approve the system's use once relevant evidence has been objectively studied, or clear indication of the system's measured need is proven, for one of the three aforesaid purposes, and following careful weighing of the above considerations.

With respect to these systems, the proposed regulation requires risk management and ethical supervision to be performed, due to the high risk involved, especially with respect to their

[46] https://www.reuters.com/article/us-eu-ai/eu-drops-idea-of-facial-recognition-ban-in-public-areas-paper-idUSKBN1ZS37Q
[47] https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence
[48] Article 5(d)

potential violation of basic rights. Additionally, the proposal refers to the need for data authentication and validation, with a strict adherence to precision of its outcomes (emphasis on preventing bias), the integration of human control in the decision-making process, maintaining system description and documentation, transparency, cyber protection and defense, instructions pertaining to suppliers and developers, financial sanctions in the event of any violations, and more.

33. **The industry** has referred to this subject on several occasions. In June of 2020 and following public criticism, a series of major companies announced that they would limit the system's use by police and law enforcement authorities, including by IBM, whose spokesperson announced that the company will stop offering, creating, and researching facial recognition technology[49]. At the same time, Microsoft announced that it would stop supplying its facial recognition technology to police, until legislation is established on the subject[50]. Furthermore, in May of 2021, Amazon announced that it would not supply its facial recognition software to police, until further notice[51], in pursuant to its June 2020 announcement on the company's suspension of its activities in this field, for a one-year period[52].

Policy Principles – The Use of Facial Recognition in Israel's Public Places

34. As indicated in the report published by the Knesset's (the Israeli Parliament's) Research Center (pages 7,10), "**There are no comprehensive and standardized policies on the distribution of video monitoring and analysis capabilities**," and "**There is no specific legislation that concretely regulates legitimate goals for the use of advanced monitoring technologies, such as facial recognition**."

The broad lack of policy and regulation pertaining to this subject, leads to the generation of a reality that is, on the one hand, unsupervised and without guidance and, on the other hand, leads to decisions or rulings being made ad-hoc, without taking the bigger picture into account.

[49] https://www.theverge.com/2020/6/8/21284683/ibm-no-longer-general-purpose-facial-recognition-analysis-software ; https://www.bbc.com/news/technology-52978191
[50] https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/
[51] https://www.reuters.com/technology/exclusive-amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18/
[52] https://news.sky.com/story/amazon-pauses-police-use-of-facial-recognition-technology-for-a-year-due-to-lack-of-laws-12004598 ; https://www.technologyreview.com/2020/06/12/1003482/amazon-stopped-selling-police-face-recognition-fight/

35. **The Biometric Applications Commissioner at the INCD believes that, in light of the dramatic improvement in the precision of facial recognition technologies, and because of the risks involved in activating facial recognition technology in public places, this subject must be regulated. Regulations should enable measured activation of these capabilities for legitimate reasons, while focusing on necessary checks and balances that take the tremendous sensitivity, risk, and potential for damage into account**.

36. The following will detail the central subjects that must be referred to, when formulating national policy on facial recognition in public places. These details must also serve as the foundation for regulating the field in primary legislation. The following principles are based on the National Policy for Biometric Applications, as well as a comparative analysis that refers to these subjects and their relevant regulations in the Western world.

Principle I: Legitimacy

When formulating policy, there is a need to examine the legitimacy of activating facial recognition capabilities in public places, and if so – under which conditions.

Upon surveying practices across the globe, it was found that there are scenarios for which the limited use of facial recognition systems in public places is deemed legitimate (for example, to prevent terror attacks[53]). Conversely, some scenarios were found to be controversial[54] (such as activating said capabilities in areas characterized by high concentrations of minors, like a schoolyard[55]).

In light of the above, it seems that the use of facial recognition in public places can be deemed legitimate in certain situations. As such, there is a need to formulate policies that limit and regulate exactly how it is executed.

Principle II: Purpose Limitation

Capturing and identifying faces in public places will be performed for limited purposes, meticulously and in accordance with relevant legislations, to ensure that the execution is aligned with its original purpose, and does not leak into other applications over time.

[53] See the EU's proposed regulation for AI, Footnote 43

[54] According to the EU's proposed legislation (see Clause 31), systems defined as being at high-risk include systems for biometric identification and classification of people that do not operate remotely and/or that **do not** operate in "real-time," or in near real-time (post).

[55] See, for example, the British Surveillance Cameras Commissioner's response, in a document outlining guidelines for police use of facial recognition in public spaces - https://bit.ly/3oUS1V3
Furthermore, the processing of information on children is one of those cases that requires an impact analysis (DPIA), in accordance with Britain's 2018 Data Protection Act - https://bit.ly/2Ks8Uri

Principle III: Proportionality

The use of image capture or facial recognition in public places will be executed in a manner than ensures balance between the advantages of using these processes, and the potential harm to individual or human rights it can cause.

Thus, for example, the EU's proposed regulation establishes that, when using real-time facial recognition systems, law enforcement officials must consider several factors, such as the degree of possible harm that could be caused, should the system not be deployed, the probability and scope of said harm taking place, as well as the ramification of the system's use on the subject's rights. To that end, it is relevant to examine the timeframe during which the system is activated, the scope and characteristics of the photographed area, the scope and type of the population being photographed (for example, minors at school), how long captured images and information is stored, etc.

Principle IV: Responsibility

Using image capture and/or facial recognition in public places must be based on pre-analyses and documented decisions by the deciding body. Documentation of the analysis must contain a weighing of alternatives for the use of such an application, including an analysis/comparison of its benefits and risks, such as privacy and security design considerations.

Emphasis should be placed on the fact that **the choice to activate the system by an outsourcing company does not remove the responsibility from the managing entity (the Controller)**.

The responsibility principle also outlines the obligation to properly manage and monitor biometric systems on an ongoing basis.

Principle V: Proper management of biometric systems

When planning and deploying the system in the field, it is important to consider technological parameters, environmental conditions, and other factors that are likely to influence the system's proper functioning and biometric comparison processes.

Among proper management musts, nondiscriminatory deployment use must be ensured (eliminating biases, such as ethnic background, gender, etc.), including the reasons and/or conditions for the system's activation, decisions made, and/or biases that pertain to its activation in the first place.

Improper activation will lead to high error and misidentification levels, which could lead to undue harm and the harassment of innocent people (including the making of false accusations), while system goals fail to be realized.
It is important that examinations be performed by objective sources who ensure that suitable standards are upheld.

The attached technological appendix includes details on these perspectives, which should be emphasized when installing and using facial recognition systems in public places.

Principle VI: Control and supervision

There is a need to define whether the use of facial recognition systems in public places requires the pre-approval of an additional, external source and, and if so, what authority should assume that position and under which conditions might their pre-approval be required. Proper and ongoing control and supervision processes must be performed on facial recognition systems in public places by an independent entity, especially with respect to data and cyber protection. This is of particular importance, as the system's results could significantly impact people's rights.

Principle VII: Cyber protection of data

Facial capture and identification in public places will be realized by using secure and reliable systems that meet necessary cybersecurity levels, so as to cope with risks such as data leakage, tampering, or misuse by unauthorized sources. It is important that these systems be planned to ensure optimal security, that suitable security tools are employed to prevent the aforesaid risks from materializing, and that ongoing control processes be upheld; when developing the system, as well as throughout its lifecycle.

The attached technological appendix includes details on these perspectives, which should be emphasized when installing and using facial recognition systems in public places.

Principle VIII: Data minimization

The biometric information that is collected and stored should be kept to an absolute minimum. Surplus information that is not absolutely necessary to achieve the desired goal should not be stored; measures should be taken to erase the collected information as soon as possible after it is processed.

This principle should be balanced against the need for proper management, which includes the gathering of quality information that will enable a low error rate to prevent the harassment of

innocent people, and the potential need for evidence to be stored, under the provisions of the law.

Principle IX: Transparency

Operators of these types of systems must let relevant populations know of their existence (information to be provided according to the circumstances surrounding the system's use), and effectively communicate information on the systems, their scope of activity, and responses to other public queries on the subject. This principle should be balanced against security considerations and protective methods, as well as against any means enacted.
Some exceptions may apply, for security reasons.

Principle X: Third-party data sharing

The starting point is that a database contains facial images captured in public places should not be shared with third parties. Data transfers can only be made to third parties upon the receipt of explicit consent from those photographed, or pursuant to judicial rulings, and other security considerations.

Principle XI: Awareness and guidance regarding privacy protection

Any entity operating facial recognition systems in public places must guide those who handle the actual facial recognition in public places (support staff, service professionals, etc.) about privacy protection and its effects on other human rights.

Conclusion

37. In recent years, facial recognition technology has dramatically improved – 100 times better than just one decade ago. This improvement, coupled with a broader distribution of security and other cameras in public places, allows facial recognition to be performed in public places at a significantly and continuously growing rate, year-over-year.
38. That said, there is a need for a comprehensive and standardized policy, and specific legislations that regulate the use of advanced monitoring technologies, such as facial recognition.
39. Due to the particular sensitivity of the subject of facial recognition in public places, as well as the unique technological perspectives of this subject, we believe that there is a need for comprehensive regulation, taking into account the principles detailed above, and that the matter should be discussed among all relevant government sources, while opening the lines for public debate as well.

Acknowledgements

The Biometric Applications Commissioner wishes to thank the INCD workers and advisors, who took part in formulating the recommendations brought forth in this document:

- Ms. Naama Ben-Zvi, Senior Head of Biometric Projects
- Mr. Michel Saguy, Scientific Director
- Mr. Yuval Segev, Director of Advanced Technology
- Mr. Zohar Ben-David, ICS Guidance Manager, Critical Infrastructures Division
- Mr. Yoav Teitelbaum, Policy Department
- Ms. Keshet Molco, Student (Research Assistant)
- Mr. Moshe Boaron, Head Engineer, Border Control, Population, and Immigration (Consultant)
- Mr. Yoram Oren, Consultant
- Mr. Avner Ben-Ephraim, Consultant
- Yuval Ne'eman Institute researchers, Tel Aviv University: Dr. Gil Baram, Ophir Harel, and Omri Wexler

Technology Appendix

(A) Deployment of a Facial Recognition System in Public Places (Cyber Considerations):

Facial capture and identification in public places will be realized by using secure and reliable systems that meet necessary cybersecurity levels, so as to cope with risks such as data leakage, tampering, or misuse by unauthorized sources. It is important that these systems are planned to ensure optimal security, that suitable security tools are deployed to prevent the aforesaid risks from materializing, and that ongoing control processes be upheld; when developing the system, as well as throughout its lifecycle.

Procedural control:

4.1 The entity's management holds primary responsibility for decision making processes pertaining to the system's deployment, means of protection, and ongoing monitoring, throughout the system's lifecycle.

4.2 Suitable and reliable testing of authorized sources must be performed.

4.3 Regular penetration testing (PT) should be considered, to ensure the system's resilience against attacks by external and internal sources alike.

Technological supervision:

4.4 A rigorous password policy should be adopted to prevent abuse, and logical, physical, and technological limitations should be placed, to enable compartmentalization and prevention of unauthorized access to the system and its data. Preference should be given to the use of strong identification mechanisms that include several factors (MFA).

4.5 It is important to implement the manufacturer's security specifications, when first activating the system, as well as throughout its lifecycle, especially with respect to allocating access permissions. Access permissions for viewing the data generated, the system itself, communications elements, and for the hardware installed in public places (cameras etc.), should be limited to relevant personal only and be as minimal as possible (on a "need to know basis").

4.6 It is preferable that the image capture system be isolated on an independent network or via a dedicated VLAN.

4.7 It is preferable that the collected biometric information (images) be stored separately/partially separate from any other personal data (belonging to that identity).

4.8 Strong commercial encryption of communications should be considered. Such encryption is critical, when internet infrastructure is deployed.

4.9 The system's software and hardware should be updated according to the manufacturer's recommendations and on secure channels only. This applies to the software updates on the operating systems, as well as to biometric applications' support systems, among others.

4.10 Physical and logical hardening of the systems should be attained, and attention should be paid to prevent physical access to the cameras (high positioning, locking, isolation, etc.).

4.11 Actions should be taken to minimize cyber risks to the supply chain, as well as to maintenance, support, and camera treatment processes, to ensure that unauthorized, third-party software is not installed on any cameras.

4.12 The manner in which the system is accessed and used by users must be monitored. In particular, abusive events enacted by system users must be identified, as should attempted breaches, and any unusual/anomalous events or patterns that digress from those that take place during regular operations. When it comes to more sensitive projects, the addition of tools of denial & deception should be considered.

(B) Proper Management of Biometric Systems (Biometric Considerations):

When planning and deploying the system, it is important to consider technological parameters, environmental conditions, and other factors that are likely to influence the system's proper functioning and biometric comparison processes.

Improper activation will lead to a high error rate and misidentification, which could lead to undue harm and the harassment of innocent people (including the making of false accusations), while system goals fail to be realized.

These technological parameters include (but are not limited to): the quality of the photo capture and information storage system; the manner in which the cameras are spread out – location, lighting, angles, focus; the quality of the biometric comparison and additional processes related to the system's operations.

When assimilating a change or correction to biometric modules, it is imperative to consult with biometric experts, rather than simply relying on QA to cover software perspectives. This, so as to ensure that changes do not lead to undesired effects on the system's performance (biometric considerations), even if the software updates operate as they should.

1. **Photo capture and data/information storage quality**

1.1. Preference should be given to the minimal resolution required for every scenario – in the case of image capture for a purpose other than facial recognition, a lower-quality

resolution that still allows the application to achieve its goal is preferable, so long as it is technologically possible.

1.2. The ongoing improvement of facial recognition engine and the potential to be able to identify at a lower resolution than the resolution used today should be considered.

1.3. When the purpose of image capture is **identification**, the optimal resolution should be calculated whilst taking into account the need for a low FPIR that will not lead to multiple false alarms and mismatches, as detailed below, as compared to its FNIR rate.

1.4. It is also imperative to consider which technological infrastructure is suitable for transferring data to the control center and then processing it, so that it does not distort the collected information.

1.5. Sanitization, the maintaining of relevant image segments by application should be performed according to the NIST SP800-88R1 standard. This is particularly relevant for image capture that is NOT intended for facial recognition purposes.

2. **Camera distribution – location, lighting, angles, and focus**

In an image capture for facial recognition purposes scenario:

2.1. Environmental conditions must be mapped to understand their influence on image capture processes.

2.2. Changing environmental conditions must be navigated: subjects' movements, distance, hidden elements, shadows or disruptive/flickering backgrounds, lighting levels (direct sunlight/darkness), various weather conditions, etc., and plan the cameras' distribution accordingly.

2.3. The optimal number of cameras required should be determined so as to, on the one hand, cover the relevant area, and, on the other hand, avoid capturing surplus information that is not needed and/or overloads the system.

2.4. The distance the camera is able to focus to must be determined, so as to define the optimal filming area and field of vision. This, so as to, on the one hand, enable relevant information to be captured, and, on the other hand, prevent surplus and unnecessary information from being collected.

3. **Biometric comparison and system operations quality**

The more sensitive/security-oriented a scenario is and the more it effects human rights, the more important the following principles will be:

3.1. A high-performance facial recognition engine (algorithm) should be selected, and a third-party examination of said algorithm is preferred (such as NIST). When a scenario

is particularly sensitive, it is recommended to use two comparison engines, and then fuse their results together (for example, by using a classic comparison engine and a DCNN, or AI-based comparison engine together).

3.2. When the scenario involves locating suspects, it is recommended to strive for as low a FPIR as possible, so as to balance operation needs with the need to reduce the false alarm rate, which would lead to the "harassment of innocent people" (by falsely matching captured subjects with identified entities included on the watchlist).

3.3. The system's error rates should be monitored and threshold calibration should be performed at regular intervals – at least once a year.

3.4. One goal should be to add as many quality images to the watchlist as possible. Controlled photographed images added to the watchlist, should meet the requirements of the ISO 19794-5 standard. "Tampered" images (edited, corrected, etc., or image segments) should not be used.

3.5. Human oversight should be integrated into the final decision-making process, once the computerized comparison has been performed. As such, it is crucial that all personnel involved in the process are suitably trained.

3.6. Reduction in the system's bias (based on gender, age, ethnic background, etc.) as much as possible is preferred. Such as system can be strived for in the following ways, among others:

3.6.1. By ensuring that the training database used to develop the comparison engine is sufficiently heterogeneous and equally represents all segments of the population.

3.6.2. By selecting a proven comparison engine that has already achieved exceptional (general) results in independent testing.

3.6.3. By periodically analyzing any false alarms, so as to oversee and improve upon the engine's performance.

3.7. Version and system updates should be performed according to the supplier's specifications.

3.8. Higher error rates should be considered, when taking into account mask wearing as a result of the Covid-19 pandemic. The system's performance in light of these conditions should be examined.

3.9. The use of liveness sensors (PAD) to identify fraud should be considered, for certain scenarios. Note that if adopted, these sensors can further infringe upon subjects' privacy, and informing the public should be weighed against security considerations.