Technical, Ethical, and Legal Considerations Regarding the Implementation of Facial Recognition in Shopping Centres

Oran Keating

December 2024

Contents

Abstract

With the integration of facial recognition technology into public spaces growing more prevalent, it is becoming increasingly important to critically examine the ethical implications of its use rather than treat it as a trivial addition to the current pool of surveillance technology to ensure its continued integration into society remains ethical. This research evaluates FRT's potential effectiveness in shopping malls as a method of footfall monitoring and enforcing banning orders, as well as highlighting key considerations for its responsible implementation by examining the legal and ethical implications of its use. This report aims to guide the council's decision-making by outlining key considerations that should be made to ensure an informed and responsible approach to FRT implementation. This report highlights the necessity of carefully balancing the benefits of the technology with its ethical challenges.

1 Introduction

Facial recognition technology (FRT) is "technology that can detect and extract a human face from a digital image then match this face against a database of pre-identified faces"[24]. FRT is becoming increasingly ubiquitous, with three-quarters of governments around the world using it on a large-scale basis, three countries in the world having no evidence of use, and two having outright banned it [4]. FRT is used most commonly in police forces, airports, and banking institutions. While its use in these institutions highlights a common theme of adoption in environments where security and verification of identities are important, how it is implemented and employed varies from institution to institution and its specific use case within [4].

Currently, three distinct types of FRT are being used [24]. One-to-one compares a single face to a set of stored faces. This type is often used for authentication, such as FaceID being used to unlock phones, integration into the IoT using FRT to lock or unlock doors [8] and its implementation into ePassports at the UK border to allow for increased throughput [25].

One-to-many compares one face against a database of other faces looking for a match [24]. This type is currently being used to help solve real-world criminal cases by correctly identifying suspects in surveillance footage [31], identifying patients in hospitals [22], [29], and could eventually be used to identify non-verbal patients in need of medical attention. This type will most likely be used to identify those violating banning orders.

The final type is inference. Its purpose is to infer attributes about a person, whether that be physical, such as race and gender, or emotional states, such as happiness or excitement [24]. (current use/future use) This type could be used in footfall monitoring to detect the kind of person most commonly found in a certain area and/or their emotional reaction to a certain stimulus, such as seeing a specific shop or product.

Due to FRT being a constantly evolving technology, the debate surrounding its legal and ethical implications is widespread and ever-changing. There is a concern that FRT, when misused, will encroach on people's privacy. Some argue that in this digital age, privacy is virtually impossible as we "live in a world in which almost everything we do, everywhere we go, and everything we buy, is recordable" [18] and that that data is more often than not "aggregated, sorted, and often sold" [18] and then used against us in an attempt to profit [32] , often violating people's rights in doing so [21].

Others argue that privacy is rapidly degrading due to misuse, suggesting that "spyware tools have often been used for illegitimate reasons, including to clamp down on critical or dissenting views and on those who express them, including journalists, opposition political figures and human rights defenders" and that most phones can easily be turned into "24-hour surveillance devices" [27]. As algorithms become increasingly good at inferring facts from seemingly unimportant data [3], [5] FRT has the potential to rapidly diminish what privacy we have left due to the sensitivity of the data it collects [13] and the inferences it can make.

Some are enthusiastic and excited by the individual and societal conveniences that FRT could bring and make suggestions as to where future areas of research should focus [1] with some choosing to demonstrate the failings of current privacy law, highlighting the need for new laws and legislation [11].

Implementing FRT in Southampton shopping centres could result in huge benefits such as increased public safety and benefits to urban development due to the footfall data collected. The problem is how FRT can be implemented effectively without encroaching on people's privacy. Failing to properly consider the challenges involved in its implementation could result in lawsuits [17], violating ethical standards, and a loss of public trust in the authorities.

Due to the numerous differing opinions on how to best implement FRT, maintaining its effectiveness while still respecting privacy, a wide range of factors from all areas must be considered, making the scale of the problem huge. As this report focuses on a specific use case, the scale of the problem diminishes to only those factors most relevant to its desired implementation. It will focus specifically on the second and third types of FRT: one-to-many matching for enforcing banning orders and inference-based systems for footfall monitoring.

The rapid advancement of FRT and its increasing ubiquity necessitate an ongoing critical examination of the legal and ethical implications of its use. Given the numerous concerns around FRT's use, it is crucial to proactively address these issues so the laws and ethical guidelines we hold ourselves to regarding its implementation do not fall behind its rapid progress. Ensuring FRT is consistently used responsibly is necessary for its continued integration into society.

2 Technical affordances and limitations

FRT has rapidly advanced thanks to its integration with deep learning technology and artificial intelligence [1]. This combination has improved FRT's performance to such an extent that it is seeing real-world use cases in police infestations and border control. However, for all of this to be successful, it must be able to perform its function effectively within the context it is applied.

2.1 The importance of training data

Much of the success of FRT is down to the data it is trained on. A good database not only increases FRT's success rate but also allows academics to reliably test and evaluate their algorithms and methods of implementation [1]. A lack of variety of datasets could result in racial discrimination, which could eventually lead law enforcement to specifically target marginalised populations [20]. It is clear that diverse and varied datasets are required both to prevent racial discrimination and to improve the success rate of FRT. This is especially important when implementing FRT in shopping centres, as the conditions are not easily controllable. This requires the data set to also have a wide range "of faces shown at different angles and exposed with different lighting conditions" [7]. The algorithms that FRT uses can either be brought pre-trained or not. While purchasing a pre-trained algorithm "may limit transparency into how these algorithms are designed and the data they are trained on" [7], training is incredibly resource intensive. For example, "Google used a dataset of 200 million facial images over four weeks to train an FRT system in 2016" [7]. Most organisations choose to not train the algorithms themselves due to the intensive computing power and amount of resources required, and while it does limit transparency, often it is not feasible. In addition, there is a risk that, if not using a pre-trained algorithm, the datasets are incorrect, missing data, or not varied enough. Whether the algorithm is pre-trained or not, it is vital that the datasets used "(i) contain a large number of persons and photographs, (ii) follow real-world requirements, and (iii) are open to the public" [1]. This will only be a concern if FRT is not brought pre-trained, as companies training it are most likely going to use a variety of correct datasets.

2.2 Current Limitations and Proposed Solution

As far as FRT has come, there are still limitations that impact its effectiveness and reliability. The limitations this report will be talking about are specific to its use case in shopping malls. While other limitations exist, they fall outside the scope of this report.

The first challenge is facial occlusions. Physical items, such as masks, glasses, or scarves; environmental factors, such as bright lights, shadows, or reflections; and positional challenges, such as facial orientation, all contribute to low recognition accuracy [1]. Environmental and positional challenges can be mitigated through testing and strategic camera placement, respectively. For example, eye-level cameras have demonstrated improved performance [2]. However, physical occlusions are much harder to address, requiring advancements in processing techniques instead of adjustments to the hardware and environment. If aware, offenders could exploit it by deliberately obscuring their faces. One possible way of limiting the impact of physical facial occlusions is to include images in the training data. The research in [1] suggests making use of the 'AR Dataset,' which includes over 3000 images of subjects with varying physical facial occlusions under various illumination conditions. For footfall monitoring, the impact of facial occlusions varies depending on the type of data you are trying to collect. For example, if people's individual reactions to specific shops are part of the desired data, facial occlusions will have a massive impact. However, if the desired data does not include anything related to people's faces, then the impact will be reduced; in this scenario you might consider if FRT is even necessary.

Another challenge is that of aging. As the gap between the reference image and an individual's current appearance grows, the accuracy of facial recognition decreases [1]. While this may not pose an issue when FRT is used for footfall monitoring, it is needed to identify those who violate banning orders, as accurately matching a face is required. One way to address this issue is to maintain an updated database of reference images by taking a new photo of offenders each year. This approach, while a valid solution, will require sustained use of resources, as the offender will need to be taken in each year.

The final challenge is that FRTs performance is mostly reliant on the conditions under which the image is acquired. As previously discussed, facial occlusions have an impact on performance, but so does the image quality.

For any type of FRT, a clear image of sufficient quality is needed to achieve reliable and accurate results [2]. Image quality relies on both the quality of the hardware and also "lighting conditions, angle of incidence, SCD, distortions, color, visibility of features, and more." [2] If the image is not of sufficient quality, the challenge of FRT significantly increases. Images with low resolutions, block artefacts, or a blur can obscure facial features or hinder the system's ability to distinguish between multiple individuals, particularly in crowded environments like shopping centers. In this context a high-quality image is necessary for FRT to function effectively [1].

To improve image quality, factors on both the hardware and software sides must be taken into account. For example, if integrating FRT directly with existing CCTV image pre-processing, it may be necessary due to CCTVs use of lossy compression potentially distorting the image [1]. Obtaining the required clear image is oftentimes much more difficult than expected. According to research conducted by [2]: "controlling for or identifying which of the multiple limiting factors contributed to the poor performance of MA would be impossible," and that even in sufficient conditions the "limiting factors cannot be isolated from one another," making it very hard to determine what is actually causing a poorer quality image. They conclude that the best way to improve the image quality, both in research and practical applications, is to have a multidisciplinary approach "with involvement from the fields of anatomy, forensic anthropology, photography, image science, and psychology, among others."

3 Ethics and the Law

3.1 The unique sensitivity of facial data

Unlike other forms of biometric data, the face is “deeply linked to personal, social, and institutional identities” [23], making the ethical issues surrounding FRT uniquely challenging. Viewing someone’s face can subconsciously influence decisions that should be driven solely by objective information, such as “criminal justice decisions” or “congressional elections” [30]. It is one of the most powerful and utilised tools in exchanging information and non-verbal communication, allowing observers to quickly and easily, and often involuntarily, make a number of inferences about a person, whether you want them to or not [14], [12]. The huge amount of diverse information a face reveals about a person makes having one’s face scrutinised a deeply personal act, and as such, the idea that a machine might do this automatically and the uncertainty of how the data captured is used makes FRT a highly contentious topic. Even if the face is not seen as personal or sensitive data, when used in combination with other information, sensitive data can be extracted through inference [28]. [28] notes this is already seen in companies ”inferring sexual orientation from music preferences”.

Due to all these factors, the ethical decisions made around the implementation of FRT are unique in their complexity and therefore must be given adequate consideration. The General Data Protection Regulation (GDPR) act recognises these complexities and challenges by classifying data to do with the face as ‘sensitive data,’ meaning it is prohibited to process unless an exception applies [16].

3.2 The ethics and practicalities of consent

One of the key exceptions under the GDPR that permits the processing of sensitive facial data is consent. Consent is a central ethical and legal consideration in regards to FRT, especially given the sensitivity of the data being collected. The ability to give informed consent is becoming increasingly difficult as more and more data is being collected about people and shared between various companies legally and illicitly [28]. One example is the Cambridge Analytica scandal, where data was collected from millions of Facebook users without their consent and used to influence elections [19]. This problem is exacerbated if the implementation of FRT is outsourced to tech giants where there is a lack of control over how the data will be processed or used. While there is no problem with outsourcing the technology, there can be no guarantee to the public that their personal data won’t be used illicitly [28]. In addition, informed consent may be impossible, as with FRT having the ability to infer and draw conclusions from received data [26] “neither the people who wrote the privacy policy nor the programmers who wrote the code for the algorithms that analyse data know what kind of inferences might be drawn” [28].

As important as the ethical concerns about consent are, it is equally important to consider the practical challenges of how consent will be obtained in a real-world setting. When FRT is used in the context of authentication, such as in FaceID, consent can be easily given; however, it becomes more challenging when implemented in public spaces. [6] found that in circumstances where FRT is implemented in public places, it is unlikely that valid consent will be able to be collected for all individuals whose data is processed, and if it is given, that it won’t be “freely given, specific, informed and unambiguous”. All these challenges suggest that consent may not be appropriate for these circumstances and that “asking for consent is misleading and inherently unfair” [6]. Having concluded that obtaining consent will be practically challenging and ethically problematic, it follows to look at other avenues where FRT can be implemented without the need of explicit consent.

Legal frameworks recognise the challenges of obtaining proper consent in these situations and, under specific circumstances, allow FRT to be used without consent being given. Under Article 6 of the GDPR, FRT can be used if the task it is performing is ‘carried out in the public interest or in the exercise of official authority vested in the controller’ and that the task has a basis in law. It must also be demonstrated that FRT is ‘a necessary and proportionate means of fulfilling the obligation or task’ [6]. For detailed guidance on how to ensure compliance with these legal requirements, resources such as [6] exist. Implementing FRT in this way is a sensible option as it ensures complete legal compliance and also deals with a lot of the ethical problems surrounding consent, as provided its use is necessary and proportional, not asking for explicit consent is justifiable.

3.3 Necessity and Proportionality

From both an ethical and legal perspective, facial recognition must be necessary and proportional to justify its use [28]. The Investigatory Powers Act of 2016 explains that proportionality must be taken into account by public authorities when making decisions that affect privacy [10]. Similarly, Article 8 of the European Convention on Human Rights (ECHR) states that public authorities can only interfere with the right to privacy if the action is ”lawful, necessary and proportionate” [9]. Employing FRT where it may not be necessary or proportional is not only ethically irresponsible but could result in legal challenges such as in the case of “Bridges v. South Wales Police,” where it was determined that the police use of FRT “was ‘not in accordance with the law’ and therefore in breach of Article 8 ECHR.” Due to all this, extra care must be given to considering FRT’s necessity and proportionality [17]. In addition, after it is employed, as the laws are constantly being updated, it must be frequently reviewed to ensure it continues to comply.

When assessing necessity, it should be taken into consideration whether the frequency of banning order violations justifies the use of FRT or if the current methods of enforcement are sufficient. Similarly, with footfall monitoring, looking at the effectiveness of current footfall monitoring methods is necessary. Considering necessity requires exploring existing solutions that achieve the same goals as FRT with less of an impact on privacy. For example, in regards to those breaking banning orders, GPS tags have been used previously to “hunt burglars and cut theft” [15], which could similarly be used to detect when people violate banning orders. In regards to footfall monitoring, less invasive methods exist, such as CCTV, electronic sensors, mobile foot printing, and kinetic pavements, which can all provide sufficient data.

When considering proportionality in its use, sensible placement of cameras could help mitigate its impact on privacy. For example, depending on what footfall data needs to be collected, only certain cameras might use FRT, such as the cameras pointing at entrances and exits to the shopping centre.

3.4 Unintended Consequences

The unintended consequences should also be taken into account when considering using FRT. If transparency is not employed when using FRT, the general public’s trust in authority may diminish. Even if transparency is employed because it is such new technology and therefore not perfect, people may feel “their ability to be treated fairly, succeed on their own merits, and receive equal justice” [23]. Alternatively, if it is ever perfected and “individuals believe they have no escape from the ubiquity of surveillance, they will be even more likely to lose trust in assurances that their data and privacy choices are being respected or enforced” [23]. This could result in people actively avoiding the area

FRT is used, creating the opposite effect than intended. The best way to mitigate this is by being completely transparent about how and why FRT is being implemented and how the collected data is being processed.

4 Conclusion

In conclusion, the integration of FRT into Southampton shopping centres has the potential to be highly effective. Its effectiveness relies on sufficient consideration of technical, legal, and ethical challenges. As demonstrated, addressing technical challenges requires a diverse team with a variety of skills, and similarly addressing ethical challenges also necessitates considering a range of viewpoints. This report concludes that due to the deeply personal and sensitive nature of the data FRT collects, extra care must be taken when considering all factors. It also concludes that logistically, consent from each individual person is too impractical to achieve; however, the law recognises this and provides adequate solutions. From a hardware perspective, it is possible to integrate FRT with existing CCTV systems in shopping centres; however, to make it as effective as possible, a multifaceted approach must be taken to its implementation. From a software side, purchasing a pre-trained algorithm is the most sensible approach for this situation, as the resources and time required to train one will most likely outweigh the benefits it brings. This report recommends that all challenges should be addressed in depth, prioritising legal compliance first, especially assessing its necessity and proportionality. This is because if it is concluded that FRT is not necessary and proportional, no other factors need to be considered. It is vital to consider pre-existing solutions rather than adamantly stick to the use of FRT. While this report tries to discuss as many relevant factors as possible, there are still technical, ethical, and legal challenges that should be looked at in detail that go unmentioned in this report.

References

[1] Insaf Adjabi et al. “Past, Present, and Future of Face Recognition: A Review”. In: *Electronics* 9.8 (2020). ISSN: 2079-9292. DOI: 10.3390/electronics9081188. URL: https://www.mdpi.com/2079-9292/9/8/1188.

[2] Nicholas Bacci et al. “Forensic Facial Comparison: Current Status, Limitations, and Future Directions”. In: *Biology* 10.12 (Dec. 2021), p. 1269. ISSN: 2079-7737. DOI: 10.3390/biology10121269.

[3] Jesús A. Ballesteros et al. “Facial emotion recognition through artificial intelligence”. In: *Frontiers in Computer Science* 6 (Jan. 2024). ISSN: 2624-9898. DOI: 10.3389/fcomp.2024.1359471.

[4] Paul Bischoff. “Facial recognition technology (FRT): Which countries use it? [100 analyzed]”. In: *Comparitech* (2021).

[5] James Coe and Mustafa Atay. “Evaluating Impact of Race in Facial Recognition across Machine Learning and Deep Learning Algorithms”. In: *Computers* 10.9 (Sept. 2021), p. 113. ISSN: 2073-431X. DOI: 10.3390/computers10090113.

[6] Information Commissioner. *The use of live facial recognition technology in public places*. Tech. rep. Information Commissioner’s Office, June 2021. URL: https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf.

[7] Centre for Data Ethics and Innovation (CDEI). *Snapshot Series Facial Recognition Technology.* Accessed: 2024-11-27. UK Government, 2020. URL: `https://assets.publishing.service.gov.uk/media/5f229fa5e90e071a56f934fb/Facial_Recognition_Technology_Snapshot_UPDATED.pdf`.

[8] Promise Elechi, Uchechukwu Ekwueme, and Ela Okowa. "Facial Recognition Based Smart Door Lock System". In: *Journal of Scientific and Industrial Research* 6 (May 2022), pp. 95–105.

[9] Equality and Human Rights Commission. "Article 8: Respect for Your Private and Family Life". In: *The Human Rights Act* (2021). URL: `https://www.equalityhumanrights.com/human-rights/human-rights-act/article-8-respect-your-private-and-family-life`.

[10] GCHQ. *Investigatory Powers Act.* GCHQ. 2019. URL: `https://www.gchq.gov.uk/information/investigatory-powers-act`.

[11] Jake Goldenfein. "Privacy's Loose Grip on Facial Recognition: Law and the Operational Image". In: *The Cambridge Handbook of Facial Recognition in the Modern State.* Ed. by Rita Matulionyte and MonikaEditors Zalnieriute. Cambridge Law Handbooks. Cambridge University Press, 2024, pp. 74–86.

[12] Judith A. Hall, Terrence G. Horgan, and Nora A. Murphy. "Nonverbal Communication". In: *Annual Review of Psychology* 70.1 (Jan. 2019), pp. 271–294. ISSN: 1545-2085. DOI: `10.1146/annurev-psych-010418-103145`.

[13] ICO. *How do we process biometric data lawfully?* Accessed: 2024-12-06 Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-process-biometric-data-lawfully/. ICO. Feb. 2024. URL: `https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-process-biometric-data-lawfully/`.

[14] Rachael E. Jack and Philippe G. Schyns. "The Human Face as a Dynamic Tool for Social Communication". In: *Current Biology* 25.14 (2015), R621–R634. ISSN: 0960-9822. DOI: `https://doi.org/10.1016/j.cub.2015.05.052`. URL: `https://www.sciencedirect.com/science/article/pii/S0960982215006557`.

[15] Ministry of Justice. *GPS tags to hunt burglars and cut theft.* UK Government. Mar. 2021. URL: `https://www.gov.uk/government/news/gps-tags-to-hunt-burglars-and-cut-theft`.

[16] KPMG. *Facial recognition Privacy considerationsin access control.* KPMG. 2021. URL: `https://assets.kpmg.com/content/dam/kpmg/nl/pdf/2021/services/facial-recognition-privacy-considerations-in-access-control.pdf`.

[17] Nora Ni Loideain. "Lawfulness and Police Use of Facial Recognition in the United Kingdom: Article 8 ECHR and Bridges v. South Wales Police". In: *The Cambridge Handbook of Facial Recognition in the Modern State.* Ed. by Rita Matulionyte and MonikaEditors Zalnieriute. Cambridge Law Handbooks. Cambridge University Press, 2024, pp. 155–172.

[18] Andrei Marmor. "Oxford Handbook of Digital Ethics". In: Oxford University Press, 2023. Chap. Privacy in Social Media, pp. 575–589. ISBN: 9780198857815.

[19] Sandra C Matz, Ruth E Appel, and Michal Kosinski. "Privacy in the age of psychological targeting". In: *Current Opinion in Psychology* 31 (2020). Privacy and Disclosure, Online and in Social Interactions, pp. 116–121. ISSN: 2352-250X. DOI: `https://doi.org/10.1016/j.copsyc.2019.08.010`. URL: `https://www.sciencedirect.com/science/article/pii/S2352250X19301332`.

[20] Alex Najibi. *Racial Discrimination in Face Recognition Technology.* Harvard University. Oct. 2020. URL: https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

[21] Neil M. Richards. "The Dangers of Surveillance". In: *Harvard Law Review* 126.7 (May 2013), pp. 1934–1965. URL: https://heinonline.org/HOL/P?h=hein.journals/hlr126&i=1965.

[22] Ayako Sadahide et al. "A Clinical Trial Evaluating the Efficacy of Deep Learning-Based Facial Recognition for Patient Identification in Diverse Hospital Settings". In: *Bioengineering* 11.4 (Apr. 2024), p. 384. ISSN: 2306-5354. DOI: 10.3390/bioengineering11040384.

[23] Evan Selinger and Brenda Leong. "590The Ethics of Facial Recognition Technology". In: *Oxford Handbook of Digital Ethics.* Oxford University Press, Dec. 2023. ISBN: 9780198857815. DOI: 10.1093/oxfordhb/9780198857815.013.32. eprint: https://academic.oup.com/book/0/chapter/337809992/chapter-ag-pdf/56877575/book_37078_section_337809992.ag.pdf. URL: https://doi.org/10.1093/oxfordhb/9780198857815.013.32.

[24] Neil Selwyn et al. "Facial Recognition Technology: Key Issues and Emerging Concerns". In: *The Cambridge Handbook of Facial Recognition in the Modern State.* Ed. by Rita Matulionyte and MonikaEditors Zalnieriute. Cambridge Law Handbooks. Cambridge University Press, 2024, pp. 11–28.

[25] Government Digital Service. *Entering the UK.* Oct. 2024. URL: https://www.gov.uk/uk-border-control/at-border-control.

[26] European Data Protection Supervisor. *TechDispatch : facial emotion recognition.* TechDispatch ... LU: Publications Office, 2021. DOI: 10.2804/519064.

[27] United Nations Human Rights Council. *Annual Report of the United Nations High Commissioner for Human Rights and Reports of the Office of the High Commissioner and the Secretary-General: Promotion and Protection of All Human Rights, Civil, Political, Economic, Social, and Cultural Rights, Including the Right to Development.* Report A/HRC/51/–. Fifty-first session, 12 September–7 October 2022, Agenda items 2 and 3. Geneva: United Nations, 2022.

[28] Carissa Véliz. "555The Surveillance Delusion". In: *Oxford Handbook of Digital Ethics.* Oxford University Press, Dec. 2023. ISBN: 9780198857815. DOI: 10.1093/oxfordhb/9780198857815.013.30. eprint: https://academic.oup.com/book/0/chapter/387347620/chapter-ag-pdf/56877020/book_37078_section_387347620.ag.pdf. URL: https://doi.org/10.1093/oxfordhb/9780198857815.013.30.

[29] Vinay Kumar Verma, Vanika Kansal, and Pankhuri Bhatnagar. "Patient Identification using Facial Recognition". In: *2020 International Conference on Futuristic Technologies in Control Systems Renewable Energy (ICFCR).* 2020, pp. 1–7. DOI: 10.1109/ICFCR50903.2020.9250002.

[30] Leslie A. Zebrowitz and Joann M. Montepare. "Social Psychological Face Perception: Why Appearance Matters". In: *Social and Personality Psychology Compass* 2.3 (Apr. 2008), pp. 1497–1517. ISSN: 1751-9004. DOI: 10.1111/j.1751-9004.2008.00109.x.

[31] De-xin Zhang, Peng An, and Hao-xiang Zhang. "Application of robust face recognition in video surveillance systems". In: *Optoelectronics Letters* 14.2 (Mar. 2018), pp. 152–155. ISSN: 1993-5013. DOI: 10.1007/s11801-018-7199-6.

[32] Shoshana Zuboff. “Social Theory Re-Wired: New Connections to Classical and Contemporary Perspectives”. In: 3rd Edition. Routledge, 2023. Chap. The Age of Surveillance Capitalism, p. 11. ISBN: 9781003320609.