Can the use of facial recognition technologies (FRTs) in law enforcement be compatible with data protection?

Dr. Francis Graydon

January 2022

Introduction

Facial recognition technologies (FRTs) are biometric systems that enable the automatic detection and recognition of a person's face.[1] The technologies have generated commercial applications from access control to 'unlocking' smart phones.[2] However, their use by law enforcement (police) is particularly controversial. In the US, there is no federal regulation of FRTs when used by law enforcement.[3] The technologies are treated with suspicion and viewed by some legal commentators as "the most dangerous surveillance tool ever invented" producing "corrosive" effects on society and call for their prohibition.[4] The contention is that their use harms privacy and creates a 'chilling effect' on constitutional rights such as freedom of association and expression.[5] Such is the level of concern about their effects, legislators in Maine, California, and Massachusetts have banned government agencies using them. Advocates and defenders of FRTs highlight the benefits and advantages to public safety and security, and emphasise the positive benefits such as crime prevention, efficient border management, and finding missing children.[6]

1. D. Yeung, R. Balebako, C. Gaviria, M. Chaykowsky (2020) 'Face Recognition Technologies: Designing Systems that Protect Privacy and Prevent Bias', p ix-x https://www.rand.org/content/dam/rand/pubs/research_reports/RR4200/RR4226/RAND_RR4226.pdf (last accessed 1 January 2022).

2. E.J Kindt 'Having yes, using no? About the new legal regime for biometric data' (2018) Computer law & security review. Jun 1;34(3):523-38, 523 https://doi.org/10.1016/j.clsr.2017.11.004 (last accessed on 11 Jan 2022).

3. E Selinger, W Hartzog 'The Case for Banning Law Enforcement from using Facial Recognition Technology' (2020) https://30glxtj0jh81xn8rx26pr5af-wpengine.netdna-ssl.com/wp-content/uploads/2020/12/20.08_Facial-Recognition-1.pdf (last accessed on 20 December 2021).

4. Ibid.

5. Ibid.

6. D. Leslie, 'Understanding bias in facial recognition technologies' (2020) p 4 https://zenodo.org/record/4050457/files/Understanding%20bias%20in%20FRT%20FINAL.pdf?download=1 (last accessed on 10 December 2021).

In the EU, the same concerns around FRTs are very evident. The European Union Agency for Fundamental Rights (EUAFR) highlights the potential 'chilling effect' of FRTs when used by police not only on rights of freedom of assembly and expression,[7] but also the threats to the fundamental right to respect for private life and data protection.[8] Despite the EU legal framework for the protection of personal data made up of the General Data Protection Directive (GDPR)[9] and the Law Enforcement Directive (LED)[10], there are concerns firstly about the effectiveness of the legal framework, and secondly about the lawfulness of police use of FRTs. In addition, the EU Commission's proposal in the Artificial Intelligence (AI) Act (April 2021)[11] to further regulate FRTs rather than ban them, may lead to legal complexities, uncertainties, and friction. The Act is criticised for enabling "population-scale surveillance" in justifiable circumstances rather than eliminating it completely. However, banning FRTs entirely would more likely eliminate the threats to personal data from police use.[12]

In addressing the question of whether police use of FRTs *can* be compatible with data protection, I will firstly examine how FRTs function and are governed by the LED and

7. European Union Agency for Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement (2020) p 29 https://ai.equineteurope.org/system/files/2021-07/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf (last accessed on 12 December 2021).

8. Ibid. p 29.

9. GDPR Regulation (EU) 2016/679 of the European Parliament and of the Council.

10. LED Directive (EU) 2016/680 of the European Parliament and of the Council.

11. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (ARTIFICIAL INTELLIGENCE ACT) and amending certain Union legislative Acts (Artificial Intelligence Act) (April 2021). https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF (last accessed on 12 December 2021).

12. M Veale and FZ Borgesius 'Demystifying the Draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach' (2021) Computer Law Review International, 22(4), 97-112, 102 https://arxiv.org/ftp/arxiv/papers/2107/2107.03721.pdf (last accessed on 16 Dec 2021).

GDPR. Secondly, I will consider some of the specific concerns that arise in complying with the relevant provisions when police process biometric data (facial images) using FRTs. Thirdly, I will highlight how the EU Commission's draft AI Act (April 2021) provides for the expansion of police use of FRTs in Member States. This will challenge the data protection legal framework and may ultimately undermine it by failing to counter-balance the threats and imbalance that will be introduced by such use.

Facial Recognition Technologies (FRTs)

Biometrics enable the identification of people through the use of distinctive biological features[13] such as (i) physiological measurements (e.g. face shape, fingerprints) or biology (e.g. DNA), or (ii) behavioural measurements (e.g. voice).[14] FRTs are a class of biometric technologies or "set of digital tools" utilised to "perform tasks on images or videos of human faces".[15] The technologies create a "biometric template" by extracting and processing biometric data.[16] FRTs are used for different purposes and involve "the automatic processing of digital images which contain the faces of individuals for the purpose of identification, authentication/verification or categorisation".[17] Facial recognition includes: (i) face detection in an image or media clip; (ii) person identification (comparing facial images to other templates stored in a

13. A. Kak, 'Regulating Biometrics: Global Approaches and Urgent Questions' AI Now Institute, (2020), ed., https://ainowinstitute.org/regulatingbiometrics.html (last accessed 3 January 2022).

14. Thales, 'Biometrics: definition, use cases, latest news' (2021) https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics (last accessed on 10 December 2021).

15. J. Buolamwini, V. Ordóñez, J. Morgenstern, and E. Learned-Miller, 'Facial Recognition Technologies: A Primer' (2020) p 2 https://globaluploads.webflow.com/5e027ca188c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf (last accessed on 1 December 2021).

16. Article 29 Working Party 'Opinion 02/2012 on facial recognition in online and mobile services' (2012) p 2 https://www.pdpjournals.com/docs/87997.pdf (last accessed on 4 January 2022).

17. Ibid.

database[18]); (iii) person verification (comparing two images of the same person[19]); and (iv) person categorisation (assessing biometric characteristics from faces e.g., race).[20]

With Live Facial Recognition Technology (LFRT) systems, person identification is based on a comparison of faces on real-time CCTV data that are mined and compared with the reference database or watchlist.[21] A significant development in FRTs is the transition to so called "Artificial Intelligence based" ('AI based') face recognition systems.[22] These systems are capable of faster, more accurate, and improved identification and the leading methodology for face detection and analysis.[23] The technology is driving and promoting the rise of real-world FRT applications.[24] The EU Commission acknowledge that the inevitable consequence of what they describe as the "second wave biometrics" is that more personal and sensitive data is collected and processed and falls within the data protection legal framework.[25] Despite this

18. Supra 13 p 30-31.

19. Ibid.

20. Supra 7 p 8.

21. P. Fussey, and D. Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology, (2019), p 19 https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf (last accessed on 4 January 2022).

22. T. Madiega and H. Mildebrath European Parliamentary Research Service(EPRS) 'Regulating facial recognition in the EU' (2021), p 2 https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf (last accessed on 3 January 2022).

23. Ibid.

24. M. Wang and W. Deng, 'Deep Face Recognition: A Survey' (2020), p 23 https://arxiv.org/pdf/1804.06655.pdf (last accessed on 3 January 2021).

25. European Commission 'Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe' (2021), p 8 https://digital-strategy.ec.europa.eu/en/library/study-supporting-impact-assessment-ai-regulation (last accessed 15 December 2021).

permitting Police use of live FRT systems provides a very powerful tool to carry out 'mass-surveillance'. The technologies enable police to collect biometric data about a person's face in a public space from a distance without the necessity of a 'police stop' or direct engagement or interaction. They provide for this surveillance in public places and the identification of people with criminal histories or other criminal difficulties who appear on a police 'watchlist'.

EU data protection legal framework

The right to the protection of personal data enshrined in the Charter of Fundamental Rights of the European Union (Article 8)[26] is a qualified right such that any limitation must be "strictly necessary" and "proportionate" pursuant to Article 52(1).[27] The EU data protection legal framework is made up of (i) the GDPR and (ii) the LED which specifically applies to law enforcement. The scope of the two legal instruments is very different but there are similarities. The obligations of data processors and data controllers are similar. In addition, the data protection impact assessment tool [28] which is so important in the planning stage of data processing is a common feature. However, compared to the GDPR, the LED has a reduced number of data subject rights.[29]

The LED sets out the legal obligations and boundaries that apply when police use FRTs. Article 3(13) LED[30] has the same definition of biometric data as 4(14) GDPR.[31] However, the processing of "biometric data for the purpose of uniquely identifying a

26. Charter of Fundamental Rights of European Union (2000/C 364/01) Article 8.

27. Ibid. Article 52(1).

28. Supra 9 Article 35 & Supra 10 Article 27.

29. M. Hudobnik, 'Data protection and the law enforcement directive: a procrustean bed across Europe?' (2020), ERA Forum 21:485–500, 486 https://doi.org/10.1007/s12027-020-00645-3 (last accessed on 6 January 2022).

30. Supra 10 Article 3(13).

31. Supra 9 Article 4(14).

natural person" is generally forbidden in the GDPR (Article 9.1)[32] but subject to exceptions (Article 9.2).[33] This "identification" prohibition is not maintained in the LED (Article 10)[34] and can be carried out: (i) for the "prevention, investigation, detection or prosecution of criminal offences"; (ii) in the "execution of penalties"; (iii) when "safeguarding against and preventing threats to public security"; and (iv) provided the data are processed by "competent authorities"[35] which encompasses police and law enforcement authorities.[36] However, under Article 10 competent authorities are permitted to process biometric data for unique identification purposes subject to a series of combined conditions: (i) where "strictly necessary" and (ii) "subject to appropriate safeguards for the rights and freedoms of the data subject" and only (iii) (a) "where authorised" by EU or Member State law" (b) "to protect the vital interests of the data subject or of another natural person" or (c) "where such processing relates to data which are manifestly made public by the data subject".[37]

Specific concerns surrounding compliance with data protection

Using FRTs involves the collection, processing, and storage of facial images automatically for the purposes of identification. The LED and the GDPR both apply to the "automated processing" of personal data and to manual processing forming part of a filing system (Article 2 LED[38] and Article 2(1) GDPR[39]). The processing of facial

32. Supra 9 Article 9.1.

33. Supra 9 Article 9.2.

34. Supra 10 Article 10.

35. Supra 10 Article 1(1).

36. Supra 7 p 3.

37. Supra 34.

38. Supra 10 Article 2.

39. Supra 9 Article 2(1).

images must comply with the key legal principles of personal data processing set out in Article 4 LED[40] and Article 5 GDPR.[41] In the LED these stipulate that processing is: (i) lawful and fair; (ii) personal data is collected for "specific", "explicit and legitimate purposes"; (iii) it must be "adequate, relevant and not excessive"; and (iv) fulfil the requirements of "accuracy", "storage "limitation, "data security and accountability".[42] In addition, data controllers should "implement appropriate technical and organisational measures" having regard to the purpose of the processing ('data protection by design and by default', Article 20 LED[43] and Article 25 GDPR[44]). Police deployment of FRTs in public places raises immediate concerns about the threats to personal data and a person's rights under the LED. These concerns centre not only on compliance with the principles of data processing highlighted above, but also the lawfulness of the processing (Article 8 LED[45]) as provided for by the Member State.

"Processed lawfully and fairly"[46]

Police use of FRTs must be lawful (Articles 4(1)(a) LED[47]) and comply with the requirements for the processing of special categories of personal data (Article 10 LED). Surveillance with FRTs may have a legal basis in national provisions under Article 8 LED. However, this has proven controversial and has been challenged in different European states.

40. Supra 10 Article 4.

41. Supra 9 Article 5.

42. Supra 40.

43. Supra 10 Article 20.

44. Supra 9 Article 25.

45. Supra 9 Article 8.

46. Supra 9 Article 4(1)(a).

47. Ibid.

In Germany, the Data Protection Authority (DPA) determined that Hamburg police had failed to establish a legal basis using video surveillance and facial images collected during the G20 Summit (2017).[48] The police biometrically processed and stored data which led to the DPA ordering the deletion of the face templates.[49] On appeal to the Administrative Court which reversed the decision, the DPA contended that Article 4(1)(a) LED had been breached because there was no legal basis to create the biometric database[50]. Furthermore, the DPA concluded that even if the legal basis applied, the use of the FRT failed to meet the requirement of "strict necessity" (Article 10 LED) and "proportionality" in accordance with established CJEU case law (Digital Rights Ireland[51] and Tele2 Sverige[52]).[53] The CJEU has set down clear and precise rules on the scope and application of the measure in question and has established minimum requirements so that data subjects have sufficient safeguards against the risks of

48. Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg, Hamburg DPA, 31 August 2018 https://datenschutz-hamburg.de/pressemitteilungen/2018/08/2018-09-31-polhh-g20-videmo360 (last accessed on 28 December 2021).

49. Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg, Hamburg DPA, 31 August 2018, p 9-27 https://datenschutz hamburg.de/assets/pdf/Antrag_Zulassung_Berufung_2020-03-13.pdf (last accessed on 11 January 2022).

50. Antrag auf Zulassung der Berufung §§ 124, 124a VwGO, Hamburg DPA, 13 March 2020, p 4-6 https://datenschutz-hamburg.de/assets/pdf/Antrag_Zulassung_Berufung_2020-03-13.pdf (last accessed on 11 January 2022).

51. C-594/12 Digital Rights Ireland and Others, paragraph 54 https://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1419450 (last accessed on 10 January 2022).

52. C-698/15 Tele 2 Sverige, paragraph 109 https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1420470 (last accessed on 10 January 2022).

53. Supra 22 p 12.

abuse.[54] The DPA has argued that the police had failed to satisfy these requirements.

The Court of Appeal for England and Wales considered the legal framework relied upon by police deploying real-time FRT in public spaces. In Bridges v The Chief Constable of South Wales Police,[55] the Court of Appeal concluded that the legal framework was fundamentally deficient. This was on the basis that too much discretion was "left to individual police officers" about "who" was to be on the 'watchlist' and "where" the FRT can be deployed".[56] Although the court did not determine the issue of proportionality, some contend the Court would have concluded that the FRT deployment was proportionate but for the failure to establish a legitimate legal basis.[57] This case in particular highlights the failures by police deploying FRTs to comply with the LED and establish a sound legal basis for processing personal data using them.

"Specific, explicit and legitimate purpose"

The provisions concerning purpose limitation (Article 4(1)(b) LED[58] and Article 5(1)(b) GDPR[59]) mandate that personal data are processed only for specific purposes and protect the data subject against data retention without limits. The EUAFR highlight that following CJEU case law, the data subject should be able to "foresee the purpose"

54. Antrag auf Zulassung der Berufung §§ 124,124a VwGO, Hamburg DPA, 13 March 2020, p 18-20 https://datenschutz-hamburg.de/assets/pdf/Antrag_Zulassung_Berufung_2020-03-13.pdf (last accessed 28 December 2021).

55. The Queen (on the application of Edward Bridges) (Appellant) v The Chief Constable of South Wales Police (Respondent) & others [2020] EWCA Civ 1058, para.153 https://www.bailii.org/ew/cases/EWCA/Civ/2020/1058.html (last accessed on 4 January 2022).

56. Ibid. para. 91.

57. Supra 53.

58. Supra 10 Article 4(1)(b).

59. Supra 9 Article 5(1)(b).

which their data will be processed.[60] Police use of FRTs may be justified in extreme circumstances involving terrorism or where there are immediate risks to public safety. This may typically be the basis of the recognised purpose limitation within EU law to allow law enforcement agencies to access a range of extensive EU records and databases.[61] However, there are legitimate concerns highlighted by the EUAFR about abuse as well as "function creep" when facial images are relied on for other purposes that were not initially foreseen.[62] Sufficient protections must be applied to ensure that FRT use is not extended and used to enter and operate with "EU large-scale databases" without a legal basis.[63]

Data Minimisation

This principle requires that personal data that is processed should be "limited" (Article 5(1)(c) GDPR[64]), or "not excessive" (Article 4(1)(c) LED[65]), to what is necessary for the purpose. Concerns complying with this mandate have been raised based on functional limitations in the technology. Firstly, the European Data Protection Supervisor (EDPS) concludes that police compliance is "highly doubtful" because FRTs are never completely accurate.[66] The algorithms used in real-time FRT systems can conceal the

60. Supra 7 p 25.

61. Ibid.

62. Ibid.

63. Ibid.

64. Supra 9 Article 5(1)(c).

65. Supra 10 Article 4(1)(c).

66. European Data Protection Supervisor 'Facial recognition: A solution in search of a problem?, 2019 https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en (last accessed on 28 Dec 2021).

biases of the programmers[67] and may result in errors in detection. Secondly, the EDPS contends that the legal requirement to comply with the accuracy principle appears to result in a never-ending collection of sensitive data to produce an "unperfectible algorithm".[68] Similarly, the CNIL (French Data Protection Authority) concluded that installing an identity system based on an FRT enabled access system breached the principles of data minimisation.[69] Police deployment of FRTs must be able to demonstrate compliance with this principle. If not, the use is illegal.

Storage Limitation

Article 4(1)(e) LED[70] and Article 5(1)(e) GDPR[71] require that personal data should not be "kept in a form that permits identification of data subjects" for "no longer than is necessary for the purposes for which the personal data are processed". Furthermore, Article 5 LED[72] stipulates that Member States propose specific time limits for storage and review. One view is the laws about the storage of certain biometric data are deficient.[73] A significant concern is that facial image databases will be retained to

67. O.A. Osoba, and W. Welser IV, 'An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence, Santa Monica, RAND Corporation, RR-1744-RC 2017. https://www.rand.org/pubs/research_reports/RR1744.html (last accessed on 7 January 2022).

68. Supra 66.

69. Commission nationale de l'informatique et des libertés, Expérimentation de la reconnaissance faciale dans deux lycées la CNIL précise sa position (2019). https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position and http://marseille.tribunal-administratif.fr/content/download/178764/1756210/version/1/file/1901249.pdf (2020) para. 13 (last accessed on 7 January 2022).

70. Supra 10 Article 4(1)(e).

71. Supra 9 Article 5(1)(e).

72. Supra 10 Article 5.

73. Supra 2 p 528.

expand continuously and used without a clear legal basis.[74] In M.K. v. France,[75] a case concerning the retention of fingerprints by police, the ECHR emphasised that personal data protection was of fundamental importance to a person's right to respect for private life. The retention amounted to disproportionate interference with the right because the national law failed to ensure the data was relevant and not excessive in relation to the purposes for which it was stored.[76] The case demonstrates the legal uncertainties created with the storage of biometric data and resulting impact on data rights. The EDPB guidance 3/2019 on "processing of personal data through video devices" under the GDPR specifies surveillance data collected for detecting vandalism should ideally be erased automatically after a few days and not stored beyond 72 hours.[77] Original data from FRTs may also need to be deleted promptly after facial templates are created.[78]

Data Accuracy

Personal data must be kept up-to-date and accurate (Article 5(1)(d) GDPR[79] and Article 4(1)(d) LED[80]). In Case C434/16 Nowak, the CJEU highlighted that the assessment of whether "personal data is accurate and complete must be made in the

74. Ibid.

75. M.K. v France, ECtHR 18 April 2013, no 19522/09. Para. 35 http://www2.bailii.org/eu/cases/ECHR/2013/341.html (last accessed on 7 January 2022).

76. Ibid. Para. 44-46.

77. European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices – version for public consultation, Brussels (2019) p 28 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf (last accessed on 28 December 2021).

78. Ibid. p 21.

79. Supra 9 Article 5(1)(d).

80. Supra 10 Article 4(1)(d).

light of the purpose for which that data was collected".[81] Compliance with this principle by police using FRTs is challenging, and it is doubted whether it can be achieved. The principle requires that input data is accurate[82] and that datasets created and relied upon to train the algorithms are representative and unbiased.[83] The EUAFR maintains that accuracy of personal data has to be understood broadly and beyond simply being correct (e.g. correct age).[84] Accuracy is also related to data quality.[85] Poor quality images can increase error, so it is incumbent on police data controllers and processors to inspect image quality and biometric templates included in watch-lists to prevent false matches.[86] A key challenge for FRT developers is using adequate system testing to find and remove accuracy inconsistencies for natural variations in gender, age, and skin colour.[87]

81. Case C434/16, Nowak, CJEU, 20 December 2017, para. 53 https://www.dataprotection.ie/sites/default/files/uploads/2018-11/20_12_17%20CJEU%20Nowak%20Judgment.pdf (last accessed on 30 December 2021).

82. European Union Agency for Fundamental Rights, 'Under watchful eyes -biometrics, EU IT-systems and fundamental rights', (2018), p 81-97 https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf (last accessed on 30 December 2021).

83. M Hildebrandt, 'The Issue of Bias. The Framing Powers of Machine Learning' (2019). Marcello Pelillo, Teresa Scantamburlo (eds.), Machine We Trust. Perspectives on Dependable AI, MIT Press 2021, https://mitpress.mit.edu/books/machines-we-trust http://dx.doi.org/10.2139/ssrn.3497597 (last accessed on 16 January 2022).

84. European Union Agency for Fundamental Rights, 'Data quality and artificial intelligence - mitigating bias and error to protect fundamental rights', (2019), p 9 https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf (last accessed on 16 January 2022).

85. Ibid.

86. Supra 84 p 12-13.

87. Council of Europe, 'Guidelines on Facial Recognition', (2021), p 9 https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3 (last accessed on 19 December 2021).

Data Security

Article 4(1)(f) LED[88] and Article 5(1)(f) GDPR[89] mandate that appropriate security measures are in place when personal data is processed. This requirement includes "protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".[90] To prevent personal data being "disclosed to" or "accessed by unauthorised individuals or organs" Article 29 LED[91] and Article 32 GDPR[92] require that the controller and processer should achieve "technical and organisational measures for ensuring the security of the processing". This should be an active ongoing process. In the guidance on the "processing of personal data on video devices", the EDPB highlight that independent of the strategy used, it is necessary for controllers and processors firstly, to "combine organisational and technical measures" to protect the system as well as the data and secondly, that this is achieved throughout the "entire lifecycle".[93] Therefore this applies from data storage (at rest), to transmission (in transit) and processing (in use).[94] Although the guidance concerns data processing under the GDPR and private individuals it should be extended to police using FRTs to ensure compliance with the LED or form part of a code of conduct.

The controller is obligated to take all necessary safeguards to keep the integrity,

88. Supra 10 Article 4(1)(f).

89. Supra 9 Article 5(1)(f).

90. Supra 88 and 89.

91. Supra 10 Article 29.

92. Supra 9 Article 32.

93. European Data Protection Board (2019), Guidelines 3/2019 on processing of personal data through video devices – version for public consultation, Brussels, 10 July 2019, p 30-31 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf (last accessed on 28 December 2021).

94. Ibid.

confidentiality and availability of the data processed.[95] The guidance is clear about the measures to reduce the risks when processing biometric data. Critically these measures should develop in tandem with advances in the technologies and include; (i) data compartmentalisation during storage and transmission, (ii) use of separate databases to store both biometric templates and raw data, (iii) encryption of biometric templates, (iv) prevention of external access to the biometric data, (v) integration of technical and organisational measures for the detection of fraud, and (vi) key management.[96] Measures centred on the deletion of raw data for face images as well as the biometric templates where a lawful basis for data processing are also suggested. In their guidelines on facial recognition, the Council of Europe also highlight critical measures that are needed to achieve data security. These also include methods aimed at (i) raw data deletion and the shortest retention periods but also focus on (ii) preventing “presentation” and “morphing attacks” on the technology itself rather than the data.[97] Further threats to data security can be anticipated because of “leakage” where police facial recognition systems interact with other IT systems.[98]

Article 20(1) LEA[99] and Article 25(1) GDPR[100] mandate that data controllers protect personal data by design. The proposed use and deployment of FRTs should be accompanied by a comprehensive analysis and plan so that the appropriate safeguards are incorporated from the outset to achieve this objective. The use of facial images by police requires a data protection impact assessment (DPIA), as well as prior consultation with the relevant data protection authority (DPA) pursuant to Articles 27-

95. Supra 93 p 21.

96. Ibid.

97. Supra 87 p 13.

98. Supra 7 p 25.

99. Supra 10 Article. 20(1).

100. Supra 9 Article 25(1).

28 (LED)[101] and Articles 35-36 (GDPR).[102] The DPIA is a particularly important tool to enable a controller to determine the legal basis and associated risks with the proposed use of FTRs. In Bridges v The Chief Constable of South Wales Police the Court of Appeal concluded that the DPIA prepared by the police for the use the automated facial recognition (AFR) technology was deficient.[103] The court found that "The DPIA failed properly to assess the risks to the rights and freedoms of data subjects and failed to address the measures envisaged to address the risks arising from the deficiencies we have found".[104]

Accountability

Data controllers are accountable for demonstrating compliance with the personal data processing principles (Article 4(4) LED[105] and Article 5(2) GDPR[106]). This places a positive "obligation" on the controller to "implement appropriate technical and organisational measures" under Article 19 and Recital 53 LED[107] and Article 24 and Recital 84 GDPR.[108] Significantly, when "new technologies" like "live FRTs" are going to be used by controllers to process personal data and there is a "high risk to the rights and freedoms of natural persons" the controller should (i) conduct a DPIA (Article 27 LED[109]) and (ii) carry out a prior consultation with the supervisory authority or data

101. Supra 10 Articles 27-28.

102. Supra 9 Articles 35-36.

103. Supra 55.

104. Ibid.

105. Supra 10 Article 4(4).

106. Supra 9 Article 5(2).

107. Supra 10 Article 19 and Recital 53.

108. Supra 9 Article 24 and Recital 84.

109. Supra 10 Article 27.

protection authority (Article 28 LED[110]). The LED and GDPR contain other key accountability tools that assist controllers in; (i) complying with the relevant provisions, and (ii) showing suitable steps have been taken to confirm compliance. Controllers are required to account for the recording of personal data processing activities (Article 24 LED[111] and Article 30 GDPR[112]) as well as documenting data breaches to the data protection agency (Article 30(5) LED[113] and Article 33(5) GDPR[114]). Enforcing stricter compliance with each of these provisions would reduce the risks to personal data.

Artificial Intelligence (AI) Act

In April 2021, the EU Commission adopted a proposal to regulate AI in the AI Act.[115] The preamble acknowledges that when the technologies are used in 'real-time' for identification purposes they risk the fundamental rights of people.[116] The legal framework proposes a classification system for AI systems that is 'risk based' and lays down different legal obligations. The regulation proposes to ban the use of AI systems for "live" or "real-time" remote biometric identification (RBI) of persons in publicly accessible spaces for the purpose of law enforcement.[117] This ban may restrict polices' arbitrary use of FRTs in public spaces and the risks to personal data with minor criminal

110. Supra 10 Article 28.

111. Supra 10 Article 24.

112. Supra 9 Article 30.

113. Supra 10 Article 30(5).

114. Supra 9 Article 33(5).

115. Supra 11.

116. Ibid. p 3.

117. Supra 11 Article 5(1)(d) and recital 33 and annex III(1)(a).

activity or public protest.[118] However, the prohibition is subject to three exceptions where the risks to fundamental rights like data protection are outweighed by a substantial public interest.[119] The three scenarios are (i) the "targeted search for potential victims of crime, including missing children" (ii) the "prevention of a specific, substantial and imminent threat to the life or physical safety of persons or of a terrorist attack" and (iii) the "detection, localisation, identification or prosecution of a perpetrator or individual suspected of a criminal offence" referred to in the European Arrest Warrant Framework Decision.[120] While 'real-time' facial recognition systems are prohibited the Act excludes: (i) "post systems" that biometrically analyse data after an event to identify individuals; (ii) systems that categorise individuals; and (iii) live biometric identification in online spaces such as video streams.[121] These are significant flaws in the proposed legislation and provide a "back door" for police to continue to use 'real-time' FRTs.

The regulation leaves it to Member States to decide whether they want to implement the exceptions for using RBI systems in their national laws.[122] The use of real-time FRTs would be subject to the principles enshrined in the LED and the GDPR. Recital 21 and Article 5(3)[123] of the proposed regulation stipulate the use shall be subject to

118. T. Christakis and M. Becuywe, Pre-Market Requirements, Prior Authorisation and Lex Specialis: Novelties and Logic in the Facial Recognition-Related Provisions of the Draft AI Regulation (2021), European Law Blog https://europeanlawblog.eu/2021/05/04/pre-market-requirements-prior-authorisation-and-lex-specialis-novelties-and-logic-in-the-facial-recognition-related-provisions-of-the-draft-ai-regulation/ (last accessed on 28 December 2021).

119. Supra 11 Article 5(1)(d).

120. Ibid.

121. M Veale and FZ Borgesius Demystifying the Draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach. Computer Law Review International, 22(4), 97-112, 101 https://arxiv.org/ftp/arxiv/papers/2107/2107.03721.pdf (last accessed on 16 Dec 2021).

122. Supra 11 Recital 22.

123. Supra 11 Recital 21 and Article 5(3).

a “prior authorisation granted by a judicial authority or by an independent administrative authority of the Member State in which the use is to take place”. The introduction of the AI Act will increase the complexity of the personal data protection regime and increase the importance of the DPA.

In response to the draft regulation, the EDPS and EDPB have significant concerns about the use of remote biometric identification and the “high risk of intrusion” into people’s private lives.[124]. They call for “a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces, including faces “in any context”.[125] Their joint opinion contends that the exceptions in the proposal are flawed because there is no adequate solution firstly, to correctly inform people about such biometric processing[126] and secondly, to safeguard a person’s timely and effective use of their data protection rights.[127] Furthermore, the use of AI systems presents serious proportionality problems”.[128] Processing biometric data involves an “indiscriminate and disproportionate number of data subjects for the identification of very few people (e.g. people in train stations).[129] The concerns raised here are valid and demonstrate the challenges and inconsistencies that will likely arise with the Act.

124. EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) p. 2-3. https://edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf (last accessed on 30 December 2021).

125. Ibid. p 3.

126. Supra 124 p 12.

127. Ibid.

128. Supra 124 p 13.

129. Supra 124 p 30.

Conclusions

The key to compatibility between police use of FRTs and data protection is to ensure compliance with the LED and the GDPR. This can further be accomplished in two distinct ways. The first is enforcing stricter compliance with the provisions discussed above by the DPA *before* FRTs are deployed. The effectiveness of this approach is demonstrated in part in the Bridges and Hamburg Police cases. However, enforcing stricter compliance needs to be strengthened through national legislation and codes of conduct[130] that clearly define the legal obligations on police. This would provide greater legal certainty and better safeguard the rights of the data subject. The second way requires the enforcement of stricter compliance and accountability *during* and *after* approved use. Stricter compliance enforcement should track the life cycle of the personal data and focus on the concerns surrounding previous failures by police to satisfy each processing principle.

The final version of the AI Act that will become law is unknown and already subject to change.[131] While it may offer the promise of greater economic benefits, the concerns expressed about AI-enabled FRTs and the threats to personal data are legitimate and real. The 'legalisation' of real-time FRTs will undermine the right to personal data protection and create a more complex and perhaps uncertain legal framework. The appropriate response to strengthening the legal framework and addressing the power imbalance that ensues should also be directed at stricter compliance enforcement by the DPA and through national legislation that further limits or bans real-time FRT use. Only then will it be possible to conclude that compatibility between police use of FRTs and data protection can be achieved.

130. Information Commissioner's Opinion 'The use of live facial recognition technology by law enforcement in public places' (31 October 2019), p 2 https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf (last accessed on 9 January 2022).

131. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. Presidency compromise text https://data.consilium.europa.eu/doc/document/ST-14278-2021-INIT/en/pdf (last accessed on 14 Jan 2022).

Bibliography

Antrag auf Zulassung der Berufung §§ 124, 124a VwGO, Hamburg DPA, (2020) https://datenschutz-hamburg.de/assets/pdf/Antrag_Zulassung_Berufung_2020-03-13.pdf (last accessed on 11 January 2022).

Article 29 Working Party 'Opinion 02/2012 on facial recognition in online and mobile services' (2012) https://www.pdpjournals.com/docs/87997.pdf (last accessed on 4 January 2022).

Buolamwini J., Ordóñez V., Morgenstern J., and E. Learned-Miller, 'Facial Recognition Technologies: A Primer' (2020) https://globaluploads.webflow.com/5e027ca188c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf (last accessed on 1 December 2021).

Case C-594/12 Digital Rights Ireland and Others https://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1419450 (last accessed on 10 January 2022).

Case C434/16, Nowak, CJEU, 20 December 2017, para. 53 https://www.dataprotection.ie/sites/default/files/uploads/2018-11/20_12_17%20CJEU%20Nowak%20Judgment.pdf (last accessed on 30 December 2021).

Case C-698/15 Tele 2 Sverige https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1420470 (last accessed on 10 January 2022).

Christakis T. and Becuywe M, Pre-Market Requirements, Prior Authorisation and Lex Specialis: Novelties and Logic in the Facial Recognition-Related Provisions of the Draft AI Regulation (2021), European Law Blog https://europeanlawblog.eu/2021/05/04/pre-market-requirements-prior-authorisation-and-lex-specialis-novelties-and-logic-in-the-facial-recognition-related-provisions-of-the-draft-ai-regulation/ (last accessed on 28 December 2021).

Commission nationale de l'informatique et des libertés, Expérimentation de la reconnaissance faciale dans deux lycées la CNIL précise sa position (2019). https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position (last accessed on 7 January 2022) and

http://marseille.tribunal-administratif.fr/content/download/178764/1756210/version/1/file/1901249.pdf (2020) (last accessed on 7 January 2022).

Council of Europe, 'Guidelines on Facial Recognition', (2021) https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3 (last accessed on 19 December 2021).

Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg, Hamburg DPA, 31 August 2018

https://datenschutz-hamburg.de/pressemitteilungen/2018/08/2018-09-31-polhh-g20-videmo360 (last accessed on 28 December 2021).

Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg, Hamburg DPA, 31 August 2018

https://datenschutz hamburg.de/assets/pdf/Antrag_Zulassung_Berufung_2020-03-13.pdf (last accessed on 11 January 2022).

European Commission ‘Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe’ (2021) https://digital-strategy.ec.europa.eu/en/library/study-supporting-impact-assessment-ai-regulation (last accessed on 15 December 2021).

European Data Protection Board (2019), Guidelines 3/2019 on processing of personal data through video devices – version for public consultation, Brussels, 10 July 2019 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf (last accessed on 28 December 2021).

European Data Protection Board -European Data Protection Supervisor Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) https://edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf (last accessed on 30 December 2021).

European Data Protection Supervisor ‘Facial recognition: A solution in search of a problem? 2019 https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en (last accessed on 28 Dec 2021).

European Union Agency for Fundamental Rights, ‘Under watchful eyes -biometrics, EU IT-systems and fundamental rights’, (2018) https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf (last accessed on 30 December 2021).

European Union Agency for Fundamental Rights, ‘Data quality and artificial intelligence - mitigating bias and error to protect fundamental rights’, (2019), p 9 https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf (last accessed on 16 January 2022).

European Union Agency for Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement (2020) https://ai.equineteurope.org/system/files/2021-07/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf (last accessed on 12 December 2021).

Fussey P. and Murray D. 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology, (2019) https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf (last accessed on 4 January 2022).

Hildebrandt M. 'The Issue of Bias. The Framing Powers of Machine Learning' (2019). Marcello Pelillo, Teresa Scantamburlo (eds.), Machine We Trust. Perspectives on Dependable AI, MIT Press 2021, https://mitpress.mit.edu/books/machines-we-trust http://dx.doi.org/10.2139/ssrn.3497597 (last accessed on 16 January 2022).

Hudobnik M. 'Data protection and the law enforcement directive: a procrustean bed across Europe?' (2020), ERA Forum 21:485–500 https://doi.org/10.1007/s12027-020-00645-3 (last accessed on 6 January 2022).

Information Commissioner's Opinion 'The use of live facial recognition technology by law enforcement in public places' (31 October 2019) https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf (last accessed on 9 January 2022).

Kak A. 'Regulating Biometrics: Global Approaches and Urgent Questions' AI Now Institute, (2020), ed., https://ainowinstitute.org/regulatingbiometrics.html (last accessed on 3 January 2022).

Kindt E.J. ‘Having yes, using no? About the new legal regime for biometric data’. (2018) Computer law & security review. Jun 1;34(3):523-38, https://doi.org/10.1016/j.clsr.2017.11.004 (last accessed on 11 Jan 2022).

Leslie D. ‘Understanding bias in facial recognition technologies’ (2020) https://zenodo.org/record/4050457/files/Understanding%20bias%20in%20FRT%20FINAL.pdf?download=1 (last accessed on 10 December 2021).

Madiega T. and Mildebrath H. European Parliamentary Research Service(EPRS) ‘Regulating facial recognition in the EU’ (2021) https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf (last accessed on 3 January 2022).

M.K. v France, ECtHR 18 April 2013, no 19522/09. http://www2.bailii.org/eu/cases/ECHR/2013/341.html (last accessed on 7 January 2022).

Osoba O.A. and Welser IV W. ‘An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence, Santa Monica, RAND Corporation, RR-1744-RC 2017. https://www.rand.org/pubs/research_reports/RR1744.html (last accessed on 7 January 2022).

Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (ARTIFICIAL INTELLIGENCE ACT) and amending certain Union legislative Acts (Artificial Intelligence Act) (April 2021). https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF (last accessed on 12 December 2021).

Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts Presidency compromise text https://data.consilium.europa.eu/doc/document/ST-14278-2021-INIT/en/pdf (last accessed on 14 Jan 2022).

Selinger E. and Hartzog W. 'The Case for Banning Law Enforcement from using Facial Recognition Technology' (2020) https://30glxtj0jh81xn8rx26pr5af-wpengine.netdna-ssl.com/wp-content/uploads/2020/12/20.08_Facial-Recognition-1.pdf (last accessed 20 December 2021).

Thales, 'Biometrics: definition, use cases, latest news' (2021) https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics (last accessed on 10 December 2021).

The Queen (on the application of Edward Bridges) (Appellant) v The Chief Constable of South Wales Police (Respondent) & others [2020] EWCA Civ 1058, para.153 https://www.bailii.org/ew/cases/EWCA/Civ/2020/1058.html (last accessed on 4 January 2022).

Veale M. and Borgesius F.Z. 'Demystifying the Draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach'. (2021) Computer Law Review International, 22(4), 97-112, https://arxiv.org/ftp/arxiv/papers/2107/2107.03721.pdf (last accessed on 16 Dec 2021).

Wang M. and Deng W., 'Deep Face Recognition: A Survey' (2020), p 23 https://arxiv.org/pdf/1804.06655.pdf (last accessed on 3 January 2021).

Yeung D., Balebako R., Gaviria C., Chaykowsky M. (2020) ‘Face Recognition Technologies: Designing Systems that Protect Privacy and Prevent Bias’, https://www.rand.org/content/dam/rand/pubs/research_reports/RR4200/RR4226/RAND_RR4226.pdf (last accessed 1 January 2022).