The compatibility of live facial recognition technology (FRT) deployment by UK law enforcement with data protection law.

Dr. Francis Graydon B.A. M.A. M.Sc. Ph.D. PGDL

Barrister

21st August 2023

INTRODUCTION

Facial recognition technologies (FRTs) are biometric systems that use artificial intelligence (AI) to enable automatic detection and identification of human faces.[1] They are on the rise internationally and deployed within a range of everyday settings. Commercial organisations in different sectors of many economies including banking,[2] security, and telecommunications[3] already exploit FRTs to offer innovative services to consumers and organisations. 'Smart cities' are developing infrastructures that include FRTs for security.[4] Law enforcement authorities (LEAs) also deploy "real-time" or "live" FRTs as remote automated policing tools in public places.[5] This application in particular has generated concerns around data protection, privacy, and state surveillance. Supporters of deployments highlight the benefits in terms of increased public safety, crime prevention, and locating lost children.[6] However, this "creep" into

[1] Douglas Yeung, et al. 'Face Recognition Technologies: Designing Systems that Protect Privacy and Prevent Bias' (2020) p ix-x https://www.rand.org/content/dam/rand/pubs/research_reports/RR4200/RR4226/RAND_RR4226.pdf (accessed 20 May 2023).

[2] Face Me Team 'How Facial Recognition Enhances Smart Banking' (2022) https://www.cyberlink.com/faceme/insights/articles/599/facial-recognition-for-smart-banking (accessed 3 June 2023).

[3] Eric Kindt, 'Having yes, using no? About the new legal regime for biometric data' (2018) Computer law & security review. Jun 1;34(3): 523, 523 https://doi.org/10.1016/j.clsr.2017.11.004 (accessed 20 May 2023).

[4] Wajeeha Ahmad & Elizabeth Dethy, 'Preventing surveillance cities: Developing a set of fundamental privacy provisions' (2019) Journal of Science Policy & Governance, 15(1) 1, 1 https://www.sciencepolicyjournal.org/uploads/5/4/3/4/5434385/ahmad_dethy_jspg_v15.pdf (accessed 25 May 2023).

[5] Ben Bowling & Shruti Iyer, 'Automated policing: The case of body-worn video' (2019) International Journal of Law in Context, 15(2), 140, 145 https://doi.org/10.1017/S1744552319000089 (accessed 25 May 2023).

[6] David Leslie, 'Understanding bias in facial recognition technologies' (2020) 4 https://zenodo.org/record/4050457/files/Understanding%20bias%20in%20FRT%20FINAL.pdf?downlo

public places has encountered strong resistance.[7] In the US, opponents call for a complete ban on deployments, [8] with some legal commentators describing the technology as “the most dangerous surveillance tool ever invented” because of the “corrosive” effects on society.[9] In the EU, the European Union Agency for Fundamental Rights (EUAFR) underscores the detrimental impact on fundamental rights to data protection and respect for private life but also the potential ‘chilling effect’ on freedom of assembly and expression.[10] UK legal commentators echo these concerns and highlight the wider societal harms[11] such as the risk of power asymmetries emerging between users and those targeted.[12]

---

ad=1 (accessed 25 May 2023).

[7] Antoaneta Roussi, 'Resisting the rise of facial recognition', 350 https://www.nature.com/articles/d41586-020-03188-2 (accessed 2 May 2023).

[8] Evan Selinger & Woodrow Hartzog ‘The Case for Banning Law Enforcement from using Facial Recognition Technology’ (2020) 6 https://theappeal.org/wp-content/uploads/2020/12/20.08_Facial-Recognition-1.pdf (accessed 20 May 2023).

[9] Ibid.

[10] European Union Agency for Fundamental Rights, ‘Facial recognition technology: fundamental rights considerations in the context of law enforcement (2020) 29 https://ai.equineteurope.org/system/files/2021-07/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf (accessed 20 May 2023).

[11] Matthew Ryder, ’Independent legal review of the governance of biometric data in England and Wales’ (2022) 7 https://www.adalovelaceinstitute.org/wp-content/uploads/2022/06/The-Ryder-Review-Independent-legal-review-of-the-governance-of-biometric-data-in-England-and-Wales-Ada-Lovelace-Institute-June-2022.pdf (accessed 25 May 2023).

[12] Centre for Data Ethics and Innovation ‘Snapshot Paper - Facial Recognition Technology’ (2020) 12-13 https://www.gov.uk/government/publications/cdei-publishes-briefing-paper-on-facial-recognition-technology/snapshot-paper-facial-recognition-technology (accessed 2 May 2023).

Live FRTs process personal data and in particular biometric data to enable the unique identification of a person.[13] Despite the concerns about the data protection and privacy risks and harms, UK law enforcement live FRT deployments are increasing[14] as evidenced from the London Metropolitan Police Service (MPS)[15] and the South Wales Police (SWP) reports.[16] A central question that arises with this ongoing development is whether these deployments can be compatible with the data protection legal framework and occupy a legitimate place within it. This '*compatibility question'* is especially relevant following the Court of Appeal decision in the Bridges case[17] and the risks identified. The question will become even more controversial with proposed changes in UK data protection law and EU law restricting AI systems use.

The focus in this dissertation is on UK law enforcement. I aim to demonstrate that live FRT deployments are complicated, legally challenging, and harmful to data protection and privacy. It is difficult to conclude that deployments are fully compatible with the data protection legal framework. Deployments create high risks of interfering with and negatively impacting these fundamental rights. A separate legal framework that properly balances the high risks and the benefits presented by the technology is required. This should provide better safeguards for data protection and privacy rights.

---

[13] European Data Protection Board Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement (26 April 2023) **(**Version 2.0) 3 https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf (accessed 27 May 2023).

[14] Metropolitan Police Service LFR deployments (2023) https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/new/lfr-deployment-grid-2023-v.3.1-web.pdf (accessed 17 June 2023).

[15] Ibid.

[16] South Wales LFR Deployments (2023) https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/live-facial-recognition/all-lfr-deployments-lleoliadau-up-to-2-july-2023.pdf (accessed 17 July 2023).

[17] *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police* [2020] EWCA Civ 1058 https://www.bailii.org/ew/cases/EWCA/Civ/2020/1058.html (accessed 20 May 2023).

I will approach the 'compatibility question' by examining how the technology must operate legally within the data protection framework. The analysis will be structured around three parts. I will first briefly explain how live FRTs process biometric data to identify a person and form the basis for law enforcement deployments. In Part 2, I will examine how law enforcement must comply with some key elements of the data protection legal framework (comprising the UK General Data Protection Regulation (UK GDPR)[18] and the Data Protection Act 2018 (DPA 2018)[19]) and also Article 8 European Convention of Human Rights (ECHRs) (right to respect for private and family life).[20] I will discuss some of the compliance problems around key data protection principles and the limitations and uncertainties in the technology to demonstrate why it is problematic to conclude deployments are framework compatible. In Part 3, I will examine the likely consequences of the UK Data Protection and Digital Information (DPDI) (No. 2) Bill [21] on deployments and the proposed restrictions in the EU through the draft AI Act.[22] Without more robust safeguards, the proposed changes may "normalise" deployments and further negatively impact data protection and privacy.

[18] UK General Data Protection Regulation

[19] Data Protection Act 2018

[20] European Convention on Human Rights (ECHR), art 8 https://www.echr.coe.int/Documents/Convention_ENG.pdf (accessed 4 January 2023).

[21] Data Protection and Digital Information (No. 2) HC Bill (2022-23) [314] https://bills.parliament.uk/bills/3430 (accessed 1 June 2023).

[22] 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), Article 5(1)(d) and recital 33 and annex III(1)(a) https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF (accessed 25 July 2023).

PART 1

FACIAL RECOGNITION TECHNOLOGIES (FRTs)

Biometrics permit person identification from their unique biological features.[23] These include physiological measurements (e.g. face shape and fingerprints), but also biology (e.g. DNA).[24] Live FRTs are a category of AI based [25] biometric technology or digital tool that process photographs and videos of human faces in specific ways.[26] This "biometric data" enables the *unique* identification of a person.[27] Human facial recognition can be understood as relying on this biometric data in a two-step process. In the first stage, the FRT system first creates a “biometric template” by taking an image of a person’s face (from an image or video) (“biometric sample”) and extracting a digital representation of its unique characteristics [28] which is stored in a database.[29] In principle, this “biometric template” with the unique characteristics in the persons

[23] Amba Kak, ’Regulating Biometrics: Global Approaches and Urgent Questions’ AI Now Institute, (2020) https://ainowinstitute.org/regulatingbiometrics.html (accessed 3 January 2023).

[24] Thales, ‘Biometrics: definition, use cases, latest news’ (2021) https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics (accessed on 19 Feb 2023).

[25] Vera Lúcia Raposo, ‘When facial recognition does not ‘recognise: erroneous identifications and resulting liabilities’ (2023) AI & Society https://doi.org/10.1007/s00146-023-01634-z (accessed 17 May 2023).

[26] Joy Buolamwini, et al, ‘Facial Recognition Technologies: A Primer’ (2020) 2 https://people.cs.umass.edu/~elm/papers/FRTprimer.pdf (accessed 1 June 2023).

[27] European Data Protection Board Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement (26 April 2023) **(**Version 2.0) 9 https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf (accessed 27 May 2023).

[28] Ibid.

[29] Ibid.

face is, over time, permanent.[30] In the second stage when facial recognition occurs, the FRT system compares the template with one or more templates that have already been created and stored or calculated directly from other "biometric samples" (images or video).[31]

Two functions of facial recognition

The facial recognition stage described above allows for two critical functions: (i) person *identification* (one template compared to many) [32] and (ii) person *authentication*. The "one-to-many identification" function can be applied to "find" a face (i.e. person) in a crowd in a public area [33] and remotely "track" the face without any physical interaction and without the persons knowledge. This can be performed without the need to establish any association with the person's name or civil identity. The objective with the second recognition stage function, authentication or "one-to-one" verification,[34] is focused on verifying that a person who presents themselves is who they claim to be.[35] The FRT system performs a comparison of a biometric template that is a pre-recorded template (e.g. stored in a biometric passport) when a *single* face is presented to the FRT system such as at an airport or border. The comparison verifies the stored template is a "match".[36] In addition to identification and verification, FRT systems also provide for person *categorisation* such as assessing biometric characteristics from

[30] Ibid.

[31] Ibid.

[32] Ibid. p 9

[33] Supra 26 p 10

[34] Supra 26 p 9

[35] Ibid.

[36] Ibid.

faces such as race.[37] It is important to highlight that both facial recognition functions are not based on an exact match between the templates but rather on an estimated match and "confidence score" between them.[38] The FRT system software does not provide a definitive result but is based only on probabilities above a system threshold and depends on the accuracy of the system software.[39] The system software is unable to determine an *exact* match (two templates belong to the same person) but only how likely it is that they belong to the same person.[40]

The distinction between the "one-to-one" and the "one-to-many" function (the latter which is used in live FRTs) is significant in terms of consent, awareness, and overall control.[41] In the former, a person typically participates directly in the process and is generally aware why and where their biometric data is processed (e.g. passport control) and usually consents to presenting their biometric data for processing. By contrast, the "one-to-many" recognition function is fundamentally different and is relied

[37] European Union Agency for Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement (2020) p 8 https://ai.equineteurope.org/system/files/2021-07/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf (last accessed on 12 December 2021).

[38] European Data Protection Board Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement (26 April 2023) (Version 2.0) 13 https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf (accessed 27 May 2023).

[39] Jane Bambauer, 'Facial recognition as a less bad option' (2021) Aegis Series Paper No. 2107. https://www.hoover.org/sites/default/files/research/docs/bambauer_webreadypdf.pdf (accessed on 2 May 2023).

[40] Commission Nationale de l'Informatique et des Libertés (CNIL) 'Reconnaissance faciale - Pour un debat à la hauteur des enjeux' (2019) https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-lahauteur-des-enjeux (accessed 27 May 2023)

[41] Information Commissioner's Opinion. The use of live facial recognition technology in public places 18 June 2021 4 https://ico.org.uk/media/for-organisations/documents/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf (accessed on 2 May 2023).

upon with live FRT deployments like the deployment of closed circuit television (CCTV) in public places such as streets and roads. In addition, live FRT deployments are typically directed on crowds of people including adults and children in a particular public location at a particular time. The FRT system automatically and indiscriminately collects vast amounts of biometric data in real time from everyone passing or stationary within the field of view of the camera.[42] This allows for the capture of biometric data from very large numbers of people on a huge scale. Based on the remote nature of how images of so many peoples' faces are captured at a distance, there is often a lack of awareness this is taking place and no real choice or control for those impacted to consent to the processing or to have any opportunity to avoid it.[43]

Law Enforcement surveillance with live FRTs

FRTs have been deployed widely for decades in sensitive public spaces in which security and public safety are perceived as being critically important. This includes airport environments where FTRs provide "face-in-a-crowd airport surveillance"[44] and at borders providing "border control passport authentication".[45] These deployments within high risk and large volume pedestrian environments in which public safety and security is vital, gives law enforcement and immigration officials a significant advantage in *identifying* known criminals or suspects, [46] as well as people on terrorist watchlists.[47] This established application of the technology demonstrates how it has

[42] Ibid.

[43] Giuseppe Mobilio, 'Your face is not new to me–Regulating the surveillance power of facial recognition technologies'. (2023) Internet Policy Review, 12(1) 2 https://doi.org/10.14763/2023.1.1699 (accessed on 29 April 2023)

[44] Supra 3 p 35

[45] Ibid.

[46] Supra 7 p 350

[47] Supra 1 p 36

become an integral part of an efficient public safety system by controlling and surveiling large numbers of people.

In recent years, FRTs have moved beyond these well protected security zones where the risks to public safety are perceived as being greater, to more public places.[48] Public places can be regarded as physical spaces outside a domestic setting, whether publicly or privately owned [49] and constitute an integral part of peoples' everyday lives and environment from which they cannot be separated. In contrast to airports or border points, public places may not need to be routinely subject to the same level of heightened security and surveillance. Despite this significant difference, it has not prevented law enforcement increasingly using live FRTs in common public places such as roads and streets.[50] The availability of live FRTs now provide law enforcement with a powerful methodology that can be deployed as part of law enforcement activities in a range of public places to overtly surveil and monitor everyone going about their lives. Live FRT deployments by law enforcement in these public places is rooted in the need to fight crime and protect the public, as well as locating vulnerable people. This trend to rely on live FRTs as an automated policing tool [51] has been interpreted

[48] Supra 3 p 35

[49] Information Commissioner's Opinion. The use of live facial recognition technology in public places 18 June 2021 4 https://ico.org.uk/media/for-organisations/documents/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf (accessed on 2 May 2023)

[50] Giuseppe Mobilio, 'Your face is not new to me–Regulating the surveillance power of facial recognition technologies'. (2023) Internet Policy Review, 12(1) 2 https://doi.org/10.14763/2023.1.1699 (accessed on 29 April 2023)

[51] Supra 5

as furthering technological innovation, but at the same time is understood to facilitate aggressive policing strategies [52] that are becoming an integral part of "new policing".[53]

UK law enforcement live FRT deployments

In the UK, the strategy to exploit live FRTs and integrate them into everyday law enforcement activities in public places is focused on London by the MPS [54] and in Cardiff by the SWP. [55] This integration began in 2017 and has been increasing. This development has proven especially controversial and exceptionally problematic because of the concerns about the risks and harms caused to data protection and privacy with the technology and the publicised failures by law enforcement to fully comply with data protection and human rights laws. This is clear from the Information Commissioner's Office (ICO) investigations of the MPS and SWP in 2019, concerning live FRT deployments.[56] This required the ICO to issue a notice to the MPS to improve governance and compliance with the data protection legal framework.[57] These events also triggered the ICO to intervene and issue specific guidance to all UK law enforcement on the use of FRTs in public places.[58] Furthermore, the decision of the

---

[52] Ibid.

[53] Jeffrey Fagan et al, 'Stops and stares: Street stops, surveillance, and race in the new policing' (2016) Fordham Urban Law Journal Vol 43, 14 https://ssrn.com/abstract=2758852 (accessed 3 May 2023).

[54] Supra 14

[55] Supra 16

[56] Information Commissioner's Annual Report and Financial Statements 2019-2020, 41 https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83- certified.pdf (accessed on 3 June 2023)

[57] Ibid. 42

[58] Information Commissioner's Opinion 'The use of live facial recognition technology by law enforcement in public places' (2019) https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf (accessed on 12 May 2023).

Court of Appeal in 2020[59] that live FRT deployments by SWP's was unlawful marks a major development and turning point in the debate.

Law enforcement now conduct overt surveillance for public protection in different settings and deploy live FRTs to achieve this.[60] The purposes of MPS's deployments in central London are broad and include; the identification of serious crime offenders, those wanted by the courts, and even people who present a "risk of harm to themselves or others".[61] Deployments use a "watchlist" of people in whom there is an interest [62] and the system generates considerable biometric data in two ways. The first is the templating of images of people on the watchlist producing biometric data.[63] The second is the templating of facial images of anyone else detected in the public place by the system camera which also produces biometric data for every face detected. [64] When the system identifies a potential "match" an alert is flagged to personnel to decide whether and what further action is required.[65] The biometric data of very large numbers of people is processed with every deployment.[66] For example, with one

[59] Supra 17

[60] Supra 14

[61] Ibid.

[62] Ibid.

[63] Metropolitan Police Service Appropriate Policy Document for sensitive data processing within Live Facial Recognition deployments (2023) 2 https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/new/mps-lfr-apd---v.2.0-web.pdf (accessed 17 June 2023).

[64] Ibid.

[65] Metropolitan Police Service LFR Policy Document Direction for the MPS Deployment of overt Live Facial Recognition Technology to locate person(s) on a Watchlist (2023) 14 https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/policy-documents/lfr-policy-document2.pdf (accessed 17 June 2023).

[66] Supra 14

central London deployment (May 2023) [67] the MPS reports only two alerts from a watchlist of 10,451 stored templates with 30,633 templates created.[68] Similarly, the SWP reports one alert from a 530 template watchlist with 130,198 templates created during a concert deployment in June 2023.[69] These extremely low alert levels are consistent with all the other deployments reported by both organisations.[70] Given the scale of the biometric data now being processed by these two large LEAs it is important to consider how they must comply with key requirements of the data protection legal framework to deploy legally land address the concerns that arise with increasing deployments.

[67] Ibid.

[68] Ibid.

[69] Supra 16

[70] Supra 14 and 16

PART 2

LEGAL FRAMEWORK

No overarching legal framework regulates live FRT deployments. Separate but overlapping provisions are engaged including data protection and human rights law implemented into domestic law but shaped by EU law. This includes decisions of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR). All live FRT deployments directly impact the right to protection of personal data (Article 8) and respect for private and family life (Article 7) under the Charter of Fundamental Rights of European Union (CFREU). [71] While the CFREU is no longer part of UK domestic law following section 5(4) European Union (Withdrawal) Act 2018,[72] UK data protection law is based on the GDPR [73] which embodies Charter Article 8. [74] Pursuant to Charter Article 52(1), any limitation to the exercise of these fundamental rights must be "necessary" and "proportionate".[75] Live FRT deployments also impact Article 8 ECHR (right to respect for private and family life).[76] The Human Rights Act 1998 (HRA) implements many rights protected by the ECHR including

[71] Charter of Fundamental Rights of European Union (2000/C 364/01), arts 7 and 8 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT (accessed 30 May 2023)

[72] European Union (Withdrawal) Act 2018, s 5(4)

[73] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation (GDPR)) [2016] OJ L119/1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 (accessed 1 April 2023).

[74] Supra 71 art 8

[75] Supra 71 art 52(1)

[76] Supra 10 p 23

Article 8.[77] Section 2 HRA [78] requires UK courts to take account of ECtHR jurisprudence and is especially important in addressing the compatibility question.

UK GDPR and DPA 2018

The UK legal framework for the protection of personal data consists of the UK GDPR[79] and DPA 2018.[80] They follow the EU data protection framework implementation made up of the GDPR[81] and Law Enforcement Directive 2016/680[82] (LED). The DPA 2018 provides for the lawful processing of personal data and "tailors" the UK GDPR.[83] In June 2021, following UK withdrawal from the EU, the EU Commission adopted two adequacy decisions for the UK (under the GDPR and the LED). It concluded the UK has an "equivalent level of protection to that guaranteed under EU law".[84] The legal

[77] Human Rights Act 1998

[78] Ibid. s 2

[79] Supra 18

[80] Supra 19

[81] Supra 55

[82] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive) [2016] L 119/89

[83] Information Commissioners Office (ICO) Guide to the UK General Data Protection Regulation (UK GDPR) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ (accessed on 29 April 2023)

[84] European Commission 'Data protection: Commission adopts adequacy decisions for the UK Brussels', 28 June 2021 https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_21_3183/IP_21_3183_EN.pdf

framework governing data processing by law enforcement is “very similar” to the one in the EU.[85] The Commission concluded the UK data protection rules in many aspects currently “closely mirror” the corresponding EU applicable rules.[86]

Part 3 DPA 2018 applies to law enforcement and implements the LED and the legal obligations for processing personal data by competent authorities for law enforcement purposes. Section 3(2) DPA 2018 [87] defines personal data as “any information relating to an identified or identifiable living individual.” Biometric data is defined as “personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allows or confirms the unique identification of that individual, such as facial images”.[88] Live FRTs process biometric data for identification and any deployment must comply with the applicable provisions. Under the GDPR, the processing of “biometric data for the purpose of uniquely identifying a natural person” is forbidden subject to exceptions.[89] This “identification”

[85] Commission Implementing Decision pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom 2021, 7, https://commission.europa.eu/system/files/2021-06/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_law_enforcement_directive_en.pdf (accessed on 29 May 2023)

[86] Commission Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, 2021, 5, https://commission.europa.eu/system/files/202106/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf (accessed on 29 May 2023)

[87] Supra 19 s 3(2)

[88] Supra 19 s 205(1)

[89] Supra 73 art 9

prohibition is not maintained in the DPA 2018[90] or the LED (Article 10).[91] Identification is permitted for law enforcement purposes including; (i) “prevention, investigation, detection or prosecution of criminal offences”; (ii) “execution of penalties”, (iii) “safeguarding against and preventing threats to public security”;[92] and (iv) provided the data are processed by “competent authorities”[93] which encompasses law enforcement.[94]

Part 3 DPA 2018 key legal requirements

The legal requirements follow a series of interconnected obligations that must be addressed individually and collectively within the data protection framework. The Information Commissioner’s Office (ICO)[95] as the “supervisory authority"[96] is also obligated to “protect the fundamental rights and freedoms” of individuals.[97] Law enforcement must comply with the six data protection principles, produce a pre-deployment policy document [98] and undertake a data protection impact assessment (DPIA).[99] Compliance with each of these obligations is necessary for lawful deployment but is a complicated process. Some obligations are more challenging and controversial than others. This is because of the complexities around the assessments

[90] Supra 19

[91] Supra 82 art 10

[92] Supra 19 s 31

[93] Supra 19 s 31(1)(b) and sch 7

[94] Ibid.

[95] Supra 18 pt 5

[96] Supra 73 art 51

[97] Supra 73 art 51(1)

[98] Supra 19 ss 35(4)(b) (5)(c)

[99] Supra 19 s 64

and judgements necessary to justify deployment. It also arises because of limitations and uncertainties in the functioning of the underlying technology that are in themselves challenges and impediments to achieving full compliance.

Data Protection Impact Assessment (DPIA)[100]

Section 64 DPA 2018 requires an impact assessment *before* any data processing is carried where it is likely to result in a high risk to the rights and freedoms of individuals.[101] This applies to live FRT deployments because biometric data is processed. The European Data Protection Board (EDPB) considers this form of processing, by itself, a serious interference, regardless of a "match" or the biometric data is deleted.[102] The ICO advises on the central importance of the DPIA to safeguard the data subject's rights and is necessary for experimental and fully operational deployment purposes. [103] Such safeguards *must* include an assessment of the risks to the rights and freedoms of data subjects [104] and include the measures envisaged to address those risks, as well as safeguards, security measures and mechanisms to ensure personal data protection and demonstrate compliance.[105] The assessment must consider the rights and legitimate interests of data subjects and other persons concerned. The ICO plays a key role in this process as law enforcement must consult with them and disclose the DPIA.[106]

[100] Ibid.

[101] Ibid.

[102] Supra 13 p 14

[103] Supra 58 p 14

[104] Supra 19 s 63(3)(b)

[105] Supra 19 ss 63(3)(c) & (d)

[106] Supra 19 s 65

The DPIA is an important safeguard increasing responsibility and promoting accountability.[107] In the Bridges case,[108] the Court of Appeal concluded the SWP DPIA failed to properly wrestle with the Article 8 HRA implications in a live FRT deployment ("AFR Locate") [109] and breached the DPA 2018. The SWP's understanding of the rights and freedoms of data subjects was flawed because they failed to properly "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" in the legal framework and required by section 64(3)(b) and (c) DPA 2018.[110]

Policy Document

Biometric data processed with live FRTs to identify an individual also constitutes "sensitive processing".[111] Sections 35(4)(b) and (5)(c) DPA 2018 stipulate that law enforcement must produce and have an "appropriate policy document" in place.[112] Section 42 DPA 2018 [113] requires firstly, the document must *explain* how the sensitive processing complies with the relevant data protection principles (s. 34(1) DPA 2018[114])

[107] Katerina Demetzou, 'Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation' (2019) Computer Law & Security Review, 35(6), 105342. https://doi.org/10.1016/j.clsr.2019.105342 (accessed 12 May 2023)

[108] Supra 17

[109] Supra 17 [153]

[110] Ibid.

[111] Supra 19 s 35(8)

[112] Supra 19 ss 35(4)(b) & (5)(c)

[113] Supra 19 s 42

[114] Supra 19 s 34(1)

(reliance on data subject consent or a Schedule 8 condition[115]).[116] Secondly, it must explain the controller's policies on retention and erasure of the personal data processed (reliance on data subject consent or a Schedule 8 condition[117]).[118] There should be an indication of how long personal data is likely to be retained. The document must be reviewed and updated from "time to time" when in place and available to the ICO. [119] Any significant change must consider the consequential risks to the data subject. The policy document like the DPIA obligates law enforcement to be accountable and responsible with live FRT deployments. The Court of Appeal did not decide on the sufficiency of the policy document in Bridges, [120] but recognised the ICO's conclusion the SWP satisfied the requirement but should have provided more detail.[121] Significantly, the court endorsed the view of the High Court [122] in deciding that it was not "necessary or desirable" to decide whether the document complied with the statutory requirements.[123] The court instead emphasised the ICO's statutory role in determining sufficiency, compliance, and providing guidance. Since the Bridges

[115] Supra 19 sch 8

[116] Supra 19 s 42(2)(a)

[117] Supra 97

[118] Supra 19 s 42(2)(b)

[119] Supra 19 s 42(3)

[120] Supra 19 [160-161]

[121] Ibid.

[122] Supra 19 [161]

[123] *R v The Chief Constable of South Wales Police and others* [2019] EWHC 2341 [141] https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf (accessed 27 May 2023)

decision, the SWP[124] and MPS[125] have completed multiple deployments. They have satisfied the ICO at least, that an "appropriate policy document" with sufficient detail has been in place at the time. While deployments appear to demonstrate an acceptable level of accountability and responsibility, [126] it is important to examine whether compliance with key data protection principles is achieved.

Data protection principles

Biometric data processed with live FRTs must comply with the six key legal principles set out at ss.35 to 40 DPA 2018[127] and Article 5 UK GDPR.[128] These interconnected principles demand that processing must be; (i) "lawful and fair",[129] (ii) collected for "specified explicit and legitimate purposes",[130] (iii) "adequate, relevant and not excessive", [131] (iv) "accurate and kept up to date",[132] (v) "kept for no longer than is

[124] Supra 16

[125] Supra 14

[126] South Wales Police 'Law enforcement processing: Part 3 Appropriate Policy Document' https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/policies-and-procedures/part_3_appropriate_policy_document.pdf (accessed 17 June 2023) AND Metropolitan Police Service Appropriate Policy Document for sensitive data processing within Live Facial Recognition deployments (2023) 6-17 https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/new/mps-lfr-apd---v.2.0-web.pdf (accessed 17 June 2023)

[127] Supra 19 ss 35 to 40

[128] Supra 18 art 5.

[129] Supra 19 s 35(1)

[130] Supra 19 s 36(1)

[131] Supra 19 s 37(1)

[132] Supra 19 s 38(1)

necessary", [133] and (vi) "processed in a secure manner".[134] Furthermore, law enforcement are required to "implement appropriate technical and organisational measures" designed to implement these principles in an effective manner considering the processing purpose.[135] The safeguards necessary for that purpose must be integrated into the processing itself and include; (a) the amount of personal data collected, (b) the extent of its processing, (c) the storage period, and (d) its accessibility. In addition, the implementation of appropriate technical and organisational measures must ensure that, *by default*, only necessary personal data for each specific processing purpose is processed ('data protection by design and by default').[136] Complying fully with these provisions and demonstrating full compliance is complicated and legally challenging. This is evident from legal challenges to deployments in the UK and EU and include the *lawfulness* of the processing and compliance failures for other principles including the technical measures employed.

"Lawful and fair"[137]

Live FRT deployments involve 'sensitive processing' of biometric data[138] and must be lawful. In the current guidelines to law enforcement on live FRT use, [139] the EDPB emphasises that under Article 52(1) of the Charter, any interference with or, restriction on the exercise of fundamental rights and freedoms recognised shall be 'provided for

[133] Supra 19 s 39(1)

[134] Supra 19 s 40(1)

[135] Supra 19 s 56.

[136] Supra 19 s 57(1)

[137] Supra 19 s 35(1)

[138] Supra 19 s 35(8)(b)

[139] Supra 27 p 20

by law'.[140] This is consistent with Article 8(2) of the ECHR which refers to "in accordance with the law".[141] In the 2019 opinion, the ICO underscores the specific conditions UK law enforcement must satisfy when deploying live FRTs.[142] Processing must be fair and "based on law" within the meaning of s.35(1) and (2) DPA 2018 [143] but also needs to be "clear, precise, and foreseeable".[144] This reflects the obligation in Article 10 LED (processing special categories of personal data)[145] which stipulates that such processing must be authorised by National laws.[146] Recital 33 LED also stresses the legal basis should be "foreseeable for those subject to it "[147] as is clear in CJEU and ECtHR decisions.[148]

In Copland v The United Kingdom the ECtHR held that to fulfil the foreseeability requirement, the law must be sufficiently clear to give individuals an adequate indication of the "circumstances in which and the conditions on which the authorities are empowered to resort to Article 8 interference".[149] In R (Catt) v Association of Chief Police Officers, the Supreme Court clarified that police powers to obtain and store

[140] Supra 71 art 52(1)

[141] Supra 20 art 8(2)

[142] Supra 58 p 7-8

[143] Supra 19 s 35(8)(b)

[144] Supra 58 p 8

[145] Supra 82 art 10

[146] Ibid.

[147] Ibid. Recital 33

[148] Ibid.

[149] *Copland v United Kingdom,* no. 62617/00, ECHR 2007- IV, para. 46 https://hudoc.echr.coe.int/eng?i=001-79996 (accessed 26 June 2023)

information for policing purposes includes common law powers [150] and this would provide a legal basis for deployment. The ICO also stresses the processing must be based either; (i) on a person giving consent *or* for the performance of a task carried out for that law enforcement purpose by a competent authority [151] *or* alternatively, (ii) on the basis the processing is 'strictly necessary' for the UK law enforcement purposes under s35(5)(a) DPA 2018,[152] while in addition, meeting a relevant condition in Schedule 8 (conditions for sensitive processing under Part 3 DPA 2018), and as required by s35(5)(b) DPA 2018.[153] Irrespective of whether "consent" is given or "strict necessity" arises, the "policy document" must be in place [154] setting out the justification for any deployment and demonstrate how the relevant conditions and the key tests of "strictly necessary" and "proportionality" are satisfied to do so lawfully. This must be completed for every deployment and cannot be predicated on practical convenience.

"Strictly necessary" threshold

Article 10 LED requires that processing of special categories of data such as biometric data can only be regarded as "strictly necessary" when the interference with the protection of personal data and its restrictions is limited to what is imperative or completely necessary. [155] This reflects the CJEU decision in the Digital Rights Ireland case where the court concluded that "derogations and limitations in relation to the

[150] *R (Catt) v Association of Chief Police Officers* [2015] UKSC 9, [2015] AC 1065 at [7] https://www.supremecourt.uk/cases/docs/uksc-2013-0112-judgment.pdf (accessed 10 May 2023).

[151] Supra 19 ss 35(2)(a) 35(4)

[152] Supra 19 s 35(5)(a)

[153] Supra 19 s 35(5)(b)

[154] Supra 19 ss 35(4)(b) 35(5)(c) 42

[155] Supra 82 art 10

protection of personal data must apply only in so far as is strictly necessary".[156] Section 35(5)(a) DPA 2018 acknowledges this and requires that, where law enforcement data perform sensitive processing *without* data subject consent, that processing must be "strictly necessary for the law enforcement purpose".[157] Strictly necessary represents a very high threshold to satisfy in the decision and planning stages of any deployment. The threshold goes well beyond being merely "necessary" pursuant to Article 52(1) of the CFREU. It acknowledges that people are being uniquely identified *without* consent and with this comes significantly higher risks to data protection and privacy which necessitates significant safeguards. Law enforcement must explain *why* the sensitive processing of biometric data with deployments satisfies this threshold.[158] The justification must form part of the "policy document"[159] and the DPIA.[160]

"Proportionality" threshold"

Law enforcement is also obligated to address the principle of *proportionality* deploying live FRT and the feasibility of using less intrusive alternatives to it.[161] In Digital Rights Ireland, the CJEU concluded that proportionality consists of "appropriateness" and

[156] Cases C-293/12 and C-594/12 *Digital Rights Ireland and Others* [2014] ECR 238, para 52 https://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1419450 (accessed 18 June 2023)

[157] Supra 152

[158] Supra 58 p 14

[159] Supra 19 ss 35(5)(a) 42

[160] Supra 99

[161] Supra 58 p 15

"necessity".[162] In Bank Mellat v HM Treasury (No 2) [163] the UK Supreme Court considered the proportionality concept. Lord Reed acknowledged its importance as a general principles of EU law and a concept applied by the ECtHR.[164] In Sporrong and Lönnroth v Sweden[165] the ECtHR determined that an essential part of the ECHR is the examination of a "fair balance between the demands of the general community interest and the requirements of the protection of the individual's fundamental rights". In the Bank Mellat case the Supreme Court explained that the "assessment of proportionality inevitably involves a value judgment at the stage at which a balance has to be struck between the importance of the objective pursued and the value of the right intruded upon".[166] Significantly the proportionality principle does not however permit the courts simply to "substitute their own assessment for that of the decision-maker".[167] The court set out the relevant principles for the *objective* justification of a limitation on a Convention right by setting out four questions [168] and is viewed as a four part proportionality test. Lord Sumption concluded that the questions depend on an "exacting analysis of the factual case advanced in defence of the measure, in order to determine (i) whether its objective is sufficiently important to justify the limitation of a fundamental right; (ii) whether it is rationally connected to the objective; (iii) whether a less intrusive measure could have been used; and (iv) whether, having regard to these matters and to the severity of the consequences, a fair balance has been struck

---

[162] Cases C-293/12 and C-594/12 *Digital Rights Ireland and Others* [2014] ECR 238, para 46 https://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1419450 (accessed 18 June 2023)

[163] *Bank Mellat v HM Treasury (No 2)* [2013] UKSC 39 https://www.supremecourt.uk/cases/docs/uksc-2011-0040-judgment.pdf (accessed 18 June 2023)

[164] Ibid. [69-70]

[165] *Sporrong and Lönnroth v Sweden* (1982) 5 EHRR 35, para 69.

[166] Supra 163 [71]

[167] Ibid.

[168] Supra 163 [20]

between the rights of the individual and the interests of the community".[169] The court considered that the four requirements are "logically separate".[170] However, in reality they will overlap due to the same facts being likely to be relevant to more than one of them.[171]

Before considering any live FRT deployment, it is incumbent on law enforcement to carefully consider each of these questions in assessing proportionality and in being able to justify the decision to go ahead with the measure. Central to any deployment decision is the key purpose behind relying on the measure and the context in which it arises. Deploying live FRTs for identification purposes to deal with serious crimes taking place in "real time" as they are happening or, to prevent an act of terrorism that is imminent and will cause loss of live and damage to property is very different to deploying live FRTs to identify known shoplifters [172] or deploying as a general methodology to identify all manner of offender in a public place. The legal requirements of "strictly necessary" and "proportionality" are more likely to be discharged when deployments are for a narrowly defined purpose, are targeted and intelligence led, and for a limited time.[173] Even this set of circumstances may not justify the deployment. The two deployment examples from the MPS and the SWP discussed above had broad deployment purposes and the scope of the identification purposes included serious crime offenders [174] but also people wanted by the courts and would likely include a wide range of criminal suspects and criminal offenders. These broad purposes and identification scope undermines the validity of the judgements made

[169] Ibid.

[170] Ibid.

[171] Ibid.

[172] Supra 58 p 15

[173] Ibid.

[174] Supra 14 and 16

before the deployment that the thresholds for “strictly necessary” and “proportionality” were validly and objectively met.

In the Bridges case at first instance, the High Court concluded the live FRT deployment was lawful and considered the four questions to be addressed on the issue of proportionality concluding that the SWP struck a fair balance between the strict necessity of data processing and the impact on individuals fundamental rights.[175] No disproportionate interference arose with Mr Bridges or anyone else’s Article 8 ECHR right.[176] With the deployment of the Live FRT on two occasions, nobody was wrongly arrested and nobody except Mr Bridges complained as to their treatment.[177] Any interference with the Mr Bridges Article 8 right would have been “very limited”.[178] However on appeal, the Court of Appeal[179] disagreed and concluded that deployment was not lawful because the legal framework had “fundamental deficiencies”.[180] The deployment failed to satisfy the requirements of Article 8(2) Human Rights Act 1998[181] and specifically the fundamental requirement of “in accordance with the law”.[182] The unlawful deployment gave two “impermissibly wide areas of discretion” to individual police officers: firstly, the selection of the people to be included on the watchlist used

[175] Supra 109 [101]

[176] Ibid.

[177] Ibid.

[178] Ibid.

[179] Supra 17

[180] Supra 17 [91]

[181] Supra 77 art 8(2)

[182] Supra 17 [152]

in the deployment (referred to by the court as the “who question”) and secondly, the location of the deployments (referred to as the “where question”).[183]

Significantly, because the court determined that the deployments were not lawful it was not required to go to determine the issue of proportionality. In addition, given that the court was dealing with an appeal, this was not a re-run of the original case but rather a consideration of whether the lower court had erred in law. However, the court did clarify that the balancing exercise with the proportionality principle necessitated “judgement by law enforcement”.[184] This approach follows the Supreme Court decision in the Bank Mellat case where the central importance of value judgments in deciding whether a balance was struck (between the rights of the individual and the interests of the community) was previously highlighted by Lord Sumption.[185] In concluding that there was a negligible impact on Mr Bridge’s Article 8 right and others in an analogous position, (where facial images were automatically deleted), the Court of Appeal focused solely on Mr Bridges right and disregarded the impact of privacy intrusions on other categories of people with the deployments. The approach of the court here was based on the pleadings in the case which highlighted the interference with Mr Bridges Article 8 right and not of everyone in the wider public who was impacted at the same time in the same way.[186] The court adopted a somewhat narrow interpretation of the scope and effect of “proportionality” assessments with live FRT deployments. The was perhaps a missed opportunity for the court to address proportionality applied to live FRT deployments more comprehensively and include the wider impact on society. In light of this decision, the approach to this assessment needs to be more tightly regulated so that it considers the intrusions on all categories of people when law enforcement is deciding whether to use live FRTs.

[183] Supra 17 [91]

[184] Supra 17 [143]

[185] Supra 163 [20]

[186] Supra 17 [142]

EU Member State decisions

Other EU Data Protection Authorities (DPA) have concluded that no legal basis exists for the deployment of live FRTs by law enforcement. The Italian DPA concluded a live FRT system ('Sari Real Time') [187] lacked a legal basis or adequate safeguards prohibiting the automated large scale processing of people not the focus of law enforcement "attention".[188] The German DPA also concluded Hamburg law enforcement failed to establish a legal basis for biometrically processing and storing facial images collected during the G20 Summit in 2017.[189] The DPA ordered the deletion of the face templates [190] which was reversed by the Administrative Court on appeal.[191] The DPA argued that even if a legal basis applied, the deployment failed the tests of "strict necessity" and "proportionality" in accordance with the CJEU

[187] Italian Data Protection Authority. Parere sul sistema Sari Real Time (2021) https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575877 (accessed 23 July 2023

[188] Ibid.

[189] 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 (accessed 28 June 2023).

[190] 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 (accessed 28 June 2023)

[191] 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 (accessed 18 June 2023)

decisions in Digital Rights Ireland[192] and Tele2 Sverige.[193] The German DPA case in particular stresses the critical importance of law enforcement correctly determining the tests of "necessity" and "proportionality" with each deployment.

"Specified, explicit and legitimate" (purpose limitation)[194]

The second principle requires that personal data are processed only for specific and explicit purposes and not further processed in a manner which is incompatible with those purposes.[195] Compliance here is critical with deployments where decisions about watchlist size and composition ("who question") [196] are made. Everyone impacted should be able to foresee the purpose for which their facial image will be processed [197] and how it is consistent with this principle. The EUAFR acknowledge live FRT may be justified in extreme circumstances involving terrorism or immediate risks to public safety. However, legitimate concerns arise with "function creep" in which watchlists are relied upon for other purposes not initially foreseen.[198] Section 36 DPA

---

[192] Cases C-293/12 and C-594/12 *Digital Rights Ireland and Others,* [2014] ECR 238, para 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 (accessed 18 June 2023)

[193] C-698/15 *Tele 2 Sverige*, [2016] ECR 970, para 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 (accessed 18 June 2023).

[194] Supra 19 s 36

[195] Ibid.

[196] Supra 17 [91]

[197] C-275/06 *Productores de Música de España (Promusicae) v. Telefónica de España SAU* [2007] ECR I-274, Opinion of AG Kokott, para. 53 https://curia.europa.eu/juris/document/document.jsf?text=&docid=62901&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1188483 (accessed 29 April 2023).

[198] Supra 10 p 25

2018 provides for any "other lawful purpose" which in addition to the legal basis requirement, must also be "necessary" and "proportionate".[199] Law enforcement cannot simply legitimise the re-use of data based on practical convenience, but must do so on re-satisfying these tests. Any re-use must be reassessed establishing a clear legal basis with the necessary safeguards and assessments. Greater transparency can be achieved here through inclusion in the policy document.

"Adequate, relevant and not excessive" [200] (data minimisation)

The data minimisation principle[201] requires that personal data processing is "limited" and "not excessive" and "relevant" to the purpose.[202] Inherent difficulties with live FRT deployments and development complying with this principle arise from the technologies underlying functionality. The European Data Protection Supervisor (EDPS) has concluded that law enforcement satisfying this principle is "highly doubtful".[203] Live FRTs may not operate accurately [204] because of built in detection error risks.[205] This potentially gives rise to the apparent "endless" acquisition of

[199] Supra 19 s 36(3)

[200] Supra 19 s 37

[201] Ibid.

[202] Ibid.

[203] 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 (accessed 23 January 2023).

[204] Ibid.

[205] Osonde Osoba and William Welser IV, 'An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence' (2017) RAND Corporation, RR-1744-RC. https://www.rand.org/pubs/research_reports/RR1744.html (accessed 27 March 2023).

excessive images to produce an algorithm that is impossible to perfect.[206] In addition, FRT systems require vast amounts of data to train and build watchlists.[207] The ICO cautions that law enforcement can follow very different practices in watchlist composition by including images of people "in the focus of police attention" targeted in operations and may indiscriminately expand the image numbers to be compared.[208] With these technical limitations and their consequences, it is difficult to accept the conclusions reached by law enforcement about data minimisation compliance are valid both by itself, and as part of "necessity" and "proportionality" assessments.

"Accurate"[209] (data accuracy)

Biometric data processed must be kept up-to-date and accurate to comply with the fourth principle.[210] The CJEU determined in C434/16 Nowak that the assessment of whether "personal data is accurate and complete must be made in the light of the purpose for which that data was collected".[211] Satisfying this principle is especially challenging with any deployment. The EUFRA highlights the different ways to evaluate and assess the accuracy of the FRT software, depending on the task and deployment purpose.[212] Even small error rates (0.01%) still means that people are incorrectly

[206] Supra 203

[207] Supra 43 p 14

[208] Supra 58 p 14-18

[209] Supra 19 s 38(1)

[210] Ibid.

[211] Case C434/16 *Peter Nowak v Data Protection Commissioner* [2017] ECR 994, para. 53 https://curia.europa.eu/juris/document/document.jsf?text=&docid=198059&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1163161 (accessed 30 June 2023)

[212] Supra 10 p 9

flagged.[213] As there are different ways to calculate and interpret error rates, this requires special attention.[214] The EDPB advises that users must consider technology reliability and accuracy to assess compliance with data accuracy.[215] This necessitates input data is accurate[216] and watchlists used to train the algorithms are representative and unbiased.[217] Bias can produce errors and inaccuracies in recognition resulting in racial, ethnic and gender discrimination.[218] Accuracy is also determined by data quality with poor images increasing error. [219] Law enforcement must inspect watchlist image and template quality to prevent errors, false positives (system identifies the wrong person) and false negatives (system fails to identify the correct person).[220]

However, the issues of accuracy and bias are especially challenging to resolve. In cases where no positive match results from the comparison, the biometric templates created should be deleted as is required by the data protection principles. However,

---

[213] Ibid.

[214] Ibid.

[215] Supra 27 p 13

[216] European Union Agency for Fundamental Rights, 'Under watchful eye -biometrics, EU IT-systems and fundamental rights', (2018), 81-97 https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf (accessed 15 January 2023).

[217] Mireille 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 (accessed 20 February 2023).

[218] Supra 43 p 17

[219] European Union Agency for Fundamental Rights, 'Data quality and artificial intelligence - mitigating bias and error to protect fundamental rights', (2019), 9 https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf (accessed 20 March 2023

[220] Ibid. p 12-13

the deletion of the template by the live FRT system immediately prevents law enforcement from carrying out any analysis or assessment of the accuracy of the biometric templates created. Similarly, the deleted data is unavailable to check and evaluate the operation and functioning of the system. Retaining the "no match" templates created during deployment is not an option as this would breach the principle of purpose limitation. This places the responsibility on the developers and demonstrates the urgent need for rigorous testing and protection against bias and discrimination to be robustly performed before any deployment. Eliminating or reducing the problem of bias in FRTs may be achieved with several strategies including; the introduction of legal standards for accuracy for the FRT systems deployed by law enforcement, improving accuracy rates across different demographics by diversifying the datasets relied upon, higher resolution image capture, increasing the diversity in the training data, as well as refining the threshold settings for different demographics to certify greater accuracy.[221] The significant challenge for FRT developers is using adequate system testing to address accuracy inconsistencies for natural variations in gender, age, and skin colour.[222] Full compliance with the principle of data accuracy and conducting valid "necessity" and "proportionality" assessments based on this can only be achieved when these technical issues are fully addressed and resolved.

"No longer than is necessary"[223] (storage limitation)

Personal data should not be "kept in a form that permits identification of data subjects" for "no longer than is necessary for the purpose for which it is processed".[224] Section

[221] Michael Mclaughlin and Daniel Castro 'The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist' (2020) 4 Available at: https://itif.org/sites/default/files/2020-best-facial recognition.pdf (accessed on 17 May 2023).

[222] Council of Europe, 'Guidelines on Facial Recognition', (2021), 9 https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3 (accessed 20 March 2023).

[223] Supra 19 s 39(1)

[224] Ibid.

39(2) DPA 2018 stipulate this is subject to specific time limits for storage and review. One criticism is that the provisions about the storage of certain biometric data are inadequate.[225] One consequence is that template databases will be preserved to grow endlessly and used continuously without a clear legal basis.[226] In the MPS policy document, controls are in place to ensure the only data retained is that which is "strictly necessary" to meet the purpose of the deployment."[227] However, it is unclear whether this test is completely satisfied with deployments. Retention for intelligence or preventative purposes is unlikely to pass a strict proportionality test, since images are stored on watchlists, without prosecution of a specific crime and without any point of closure. In M.K. v. France,[228] concerning the retention of fingerprints by police, the ECtHR emphasised that personal data protection was of fundamental importance to a person's right to respect for private life. Retaining the prints constituted a disproportionate interference with this right as French law failed to ensure the data was relevant and not excessive in relation to the purposes for which it was stored.[229] Storage limitation is especially critical with live FRT deployments because it supports any test of proportionality imposing certainty and a final limit on data processing.

[225] Supra 3 p 523

[226] Ibid. 528

[227] Supra 63 p 15

[228] *M.K. v France,* no.19522/09, ECHR 2013-V https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-119075&filename=001-119075.pdf (accessed 23 June 2023)

[229] Ibid. [44-46]

"Processed in a secure manner"[230] (data security)

The sixth data protection principle mandates personal data processed for any law enforcement purpose must be subject to "appropriate security measures". [231] This includes "protection against unauthorised or unlawful processing and against accidental loss, destruction or damage" [232] To comply with this principle, "appropriate technical and organisational measures" must be implemented in an effective way which must be integrated into the processing itself.[233] Details of these measures must be included in the policy document. The ICO emphasises the overall importance of privacy by design and default to comply with this principle.[234] The data security process must change to reflect the dynamic nature of deployments[235] and the data lifecycle must be considered.[236] This is consistent with other EDPB guidance for processing personal data on video devices where storage (at rest), transmission (in transit) and use (processing) stages are identified. Measures to reduce the risks with biometric data processing include; compartmentalisation, reliance on different databases, template encryption and preventing external access to the data. [237] Measures centred on raw data deletion for face images and templates are particularly

[230] Supra 19 s 40

[231] Ibid.

[232] Ibid.

[233] Supra 19 s 57

[234] Supra 41

[235] European Data Protection Board Guidelines 3/2019 on processing of personal data through video devices – version for public consultation (2019) 30-31 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf (accessed 24 June 2023).

[236] Ibid.

[237] Ibid.

effective and are currently used with deployments by law enforcement.[238] However, other data security threats include “leakage” when live FRTs interact with other IT systems.[239] This is an issue that may become increasingly more important with the expansion of deployments and the strategy aimed at expediting it.

Having discussed some of the problems around compliance with key elements of the DPA 2018, it is important to now consider the importance of Article 8 ECHR as an integral part of the data framework with all deployments.

Article 8 ECHR

The notion of ‘private life’ within Article 8 ECHR (right to respect for private and family life) includes the collection and retention of biometric data based on previous decisions of the ECtHR. Live FRT deployments directly impact this right.[240] In S and Marper v United Kingdom[241] which concerned the collection and retention of DNA and fingerprint (biometric data) data, the court concluded the “protection of personal data is of fundamental importance to a person’s enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention”.[242] The collection of an individual’s’ biometric data “allowing his or her identification with precision in a wide range of circumstances’ is, capable of affecting his or her private life and gives

[238] Supra 63 p 15

[239] Supra 219 p 2

[240] Supra 10 p 23.

[241] *S and Marper v United Kingdom,* nos. 30562/04 and 30566/04 [2008] ECHR https://hudoc.echr.coe.int/eng?i=001-90051 (accessed 20 July 2023)

[242] Ibid. [103]

rise 'to important private-life concerns".[243] In Aycaguer v France [244] a case concerning DNA retention, the court considered that "personal data protection plays a primordial role in the exercise of a person's right to respect for his private life enshrined in Article 8 of the Convention".[245] Where a particularly important aspect of identity is in issue, the state's allowable margin of appreciation is generally narrower when assessing whether interference was necessary.[246]

In Gaughran v Chief Constable of Northern Ireland [247] concerning biometric data retention (DNA, fingerprints, and photograph), the ECtHR held that the implementation of facial recognition tools and using images captured during a person's arrest and stored for an indefinite time breached Article 8. Law enforcement failed to strike a fair balance between the competing public and private interests.[248] The retention of the biometric data constituted a "disproportionate interference with the applicant's right to respect for private life" [249] and could not be regarded as "necessary in a democratic society".[250] The decision in Gaughran is especially relevant when considering live FRT deployments. It challenges how relying on broad deployment purposes and retaining watchlists of persons of interest, can be justified as "necessary" and "proportionate" and not constitute a disproportionate interference with the Article 8 right of all those

[243] Ibid. [84-86]

[244] *Aycaguer v. France* no. 8806/12 ECHR, 2017-V https://hudoc.echr.coe.int/eng?i=001-174441 (assessed May 2023)

[245] Ibid. [38]

[246] Ibid. [37]

[247] *Gaughran v Chief Constable of Northern Ireland*, no. 45245/15 ECHR 2020-I https://hudoc.echr.coe.int/eng?i=001-200817 (accessed 3 July 2023)

[248] Ibid. [96]

[249] Ibid. [97]

[250] Ibid.

impacted. Without tighter regulation on law enforcement around their discretion about "who" and "where" identified in Bridges[251] the risks of breaching Article 8(2) HRA 1998 [252] and not "in accordance with the law" [253] will be greater with further deployments.

[251] Supra 17 [91]

[252] Supra 77 art 8(2)

[253] Supra 17 [152]

PART 3

NEW DATA PROTECTION FRAMEWORK

The UK data protection legal framework will change in the coming years. At this stage it is premature to conclude what the new framework will eventually look like when it is finalised and passed into law. However, it is still important and relevant at this stage to consider the potential effects of some of the current proposals on law enforcement's ongoing strategy of live FRT deployments. Equally, it is also important to consider the potential effects of the proposed changes on data protection and privacy rights. In addition, the effects of the proposed changes on live FRT deployments by UK law enforcement also need to be considered alongside proposed changes in the EU restricting the use of AI systems. [254] The EU draft AI Act [255] sets out a harmonised legal framework for the development, supply and use of AI products and services in the EU. While the Act has not yet come into law and the final version is yet to be determined, it will likely have the effect of introducing restrictions on live FRT deployments by EU law enforcement.

UK Data Protection and Digital Information (No. 2) Bill (DPDI2) [256]

In March 2023, the UK Department for Science, Innovation and Technology (DSIT) published the Data Protection and Digital Information (No. 2) Bill (DPDI2).[257] The Bill, described by government as creating "a new UK data rights regime tailor-made"[258] for

[254] Supra 22

[255] Ibid.

[256] Supra 21

[257] Ibid.

[258] Introduction of the Data Protection and Digital Information (No. 2) Bill Statement made on 8 March 2023 by Michelle Donellan

UK needs is significant and will change the data protection landscape for several reasons. Firstly, it represents law makers first effort since the UK's EU withdrawal to reform data protection laws and introduce a UK independent data protection legal framework. Secondly, the Bill objective is focused on eliminating uncertainty and on "better data access" and "better use of personal data" [259] rather than the aim of introducing a framework that strengthens and improves data protection and privacy rights in the changing and ever more complex "digital landscape".[260] The focus on better use of data is considered "fundamental to economic growth, scientific research, innovation, and increasing productivity."[261] The third reason why the Bill is important is that it proposes significant changes to key elements of the current data protection legal framework to achieve this. The overall effect of the Bill has been criticised because it does no more than amend rather repeal the current data protection framework.[262] In addition, this strategy has also been criticised in the House of Lords as simply giving rise to "a series of patchwork amendments" which will further confuse and complicate what is already an "overcomplex" area of legislation.[263] The legislation is still making its way through Parliament and although the final version will have to be decided by law makers it is important to consider proposed changes that will impact the use of live FRTs by law enforcement.

---

https://questions-statements.parliament.uk/written-statements/detail/2023-03-08/hcws617 (accessed 6 June 2023)

[259] Ibid.

[260] Ibid.

[261] Ibid.

[262] Big Brother Watch Briefing on the Data Protection and Digital Information 2.0 Bill for House of Commons Committee Stage (2023) 7 https://bigbrotherwatch.org.uk/wp-content/uploads/2023/05/Big-Brother-Watch-Briefing-on-the-Data-Protection-and-Digital-Information-2.0-Bill-for-House-of-Commons-Committee-Stage.pdf (accessed 5 June 2023)

[263] Lord Collins of Highbury speaking in the House of Lords (23 March 2023) https://parliamentlive.tv/Event/Index/39ad3b3f-46c4-4408-882a-a6d1694496d8

The Bill [264] introduces several amendments that are directly relevant to the use of live FRTs by law enforcement. The effect of the changes would potentially eliminate or lessen the current set of legal obligations on law enforcement when deploying live FRTs as discussed above. This would weaken the existing data protection and privacy protections. Three proposed amendments are especially noteworthy and particularly relevant to this discussion; (i) change to definition of personal data, (ii) automated decision making (ADM), and (iii) codes of practice. A significant change to the definition of personal data is proposed. Bill Clause 1[265] introduces a significant change to the current definition of personal data under s.3(2) DPA 2018 ("any information relating to an identified or identifiable living individual")[266] and restricts it by introducing a "directly or indirectly" distinction.[267] Under Bill Clause 1(2) data only qualifies as personal data if it relates to an individual who is identifiable by a data controller/processor by "reasonable means at the time of the processing" or alternatively if the controller ought to "reasonably know" that another person will be able to obtain the information as a result of the processing and identify the individual "by reasonable means" at the time of processing. [268]

The ICO, in formally responding to the government's consultation under Article 36(4) UK GDPR[269] concludes that there is no evidence of any cases where information previously caught by the current definition would not be caught by the new definition.[270]

---

[264] Supra 21

[265] Ibid. cl 1

[266] Supra 19 s 3(2)

[267] Supra 19 s 3(3)

[268] Supra 21 cl 1(2)

[269] Supra 18 art 36(4)

[270] Information Commissioner's Response to the Data Protection and Digital Information (No 2) Bill (DPDI No 2 Bill) (2023) 9 https://ico.org.uk/media/about-the-ico/consultation-responses/4025316/response-to-dpdi-bill-20230530.pdf (accessed 5 June 2023)

However, despite this analysis the ICO also highlights that the definition change is still potentially confusing and gives rise to potential privacy risks.[271] In contrast to the ICO's conclusion, in its submissions to the consultation Big Brother Watch criticises the proposed definition change. [272] They conclude that effect of the change will be the application of a less stringent test for what qualifies as personal[273] and result in increased levels of data processing with reduced or no levels of protection.[274] Both these criticisms are valid and the change may introduce a mechanism to shift personal data that is currently protected to being unprotected.

The potential practical effect of the revised definition of personal data on live FRTs deployment by law enforcement is especially significant. The data protection legal obligations and protections would likely only apply if people were on the FRT watchlist compiled by law enforcement but would *not* apply to individuals who are not on the watchlist and whose personal data (biometric template) is deleted immediately after it is processed because it does not return a match.[275] This has been interpreted as providing a methodology to shift future live FRT deployments by law enforcement to a position outside of the UK GDPR obligations and into a zone of "uncertainty". This effects risks creating a data protection regime that lacks transparency. [276] At the same time this would also increase the discretion enjoyed by law enforcement with respect

---

[271] Ibid.

[272] Ibid. p 7

[273] Ibid.

[274] Ibid.

[275] Chris Pounder 'Facial recognition CCTV excluded from new data protection law by definition of "personal data"' (2023) https://amberhawk.typepad.com/amberhawk/2023/04/facialrecognition-cctv-excluded-from-new-data-protection-law-by-definition-of-personal-data.html (accessed 5 June 2023)

[276] Ibid.

to the “who” and “where” of deployments. This would potentially result in less law enforcement accountability and expedite the “normalisation” of live FRT deployments throughout UK society.

A second area likely to influence decisions about live FRT deployments by law enforcement is proposed changes to the scope of automated decision making (ADM). In the Bridges case the Court of Appeal highlighted that personal data was processed by the live FRT in an automated way but also involved some human intervention after a match occurred.[277] The goal of the current Bill is to make it more possible for law enforcement to use ADM technology.[278] Bill Clauses 11(2) and (3) propose to replace the general prohibition on ADM by law enforcement with a general prohibition only on ADM processing special category personal data (proposed s.50B).[279] The exceptions would apply when data subject give “explicit consent” [280] or where “the decision is required or authorised by law”.[281] Any changes that include ADM will clearly engage the ECHR because of the potential to negatively impact the right to privacy and respect for private live. The ICO’s response to the consultation concludes that the aim of making ADM simpler is welcomed [282] but surprisingly does include any conclusions on the potential effects on privacy. The effect of this change on live FRT deployments is potentially very significant. Law enforcement may interpret the scope of the exception “authorised by law” more widely and continue to rely on the common law as

[277] Supra 17 [89] [184]

[278] Data Protection and Digital Information (No. 2) Bill: European Convention on Human Rights Memorandum (8th March 2023) 9 https://publications.parliament.uk/pa/bills/cbill/58-03/0265/echrmemo.pdf (accessed 5 June 2023).

[279] Supra 21 s 50B

[280] Supra 21 s 50B(2)

[281] Supra 21 s 50B(3)

[282] Supra 270 p 4

is currently the case [283] and live FRT deployments the SWP and the MPS. Without specific legal provisions that apply to live FRTs deployments by law enforcement increased use and reliance on ADM would face few restrictions.[284] This would potentially encourage and facilitate increased and more routine deployments. While this could increase public security it will have the effect of significantly increasing the risks and harms to data protection and privacy which the Bill acknowledges[285] exist including interference with Article 8 ECHR.

The third amendment in the Bill that may have an effect on how law enforcement deploys live FRTs centres on the introduction of codes of conduct. Clause 19 (law enforcement processing and codes of conduct) introduces for the first time provisions to produce codes of conduct to demonstrate compliance with the legal requirements surrounding the processing of personal data by law enforcement. The Bill specifies that the code of conduct make provision about; (a) "lawful and fair processing" (b) the collection of personal data; (c) the information provided to the public and to data subjects; (d) the exercise of the rights of data subjects; and (e) the data protection by design and default measures and procedures and logging.[286] While the Bill mandates that the ICO must encourage expert public bodies to produce the codes of conduct intended to contribute to compliance and additionally must approve these codes, the Bill does not mandate that they are used by controllers such as law enforcement to demonstrate compliance [287] rendering it somewhat ineffective.

---

[283] Supra 262

[284] Ibid. p 23.

[285] Impact Assessment Data Protection and Digital Information (No. 2) Bill: European Convention on Human Rights Memorandum https://www.gov.uk/government/publications/data-protection-and-digital-information-bill-impact-assessments/data-protection-and-digital-information-no-2-bill-european-convention-on-human-rights-memorandum (accessed 5 June 2023)

[286] Supra 21 s 68A

[287] Ibid.

Overall, these three proposed changes may potentially create a more “permissive” data protection regime that encourages routine live FRT deployments by law enforcement. This may lead to facial recognition becoming more normalised in UK society. At the same time this would continue to have greater detrimental effects on eroding existing data protection and privacy rights.

EU draft Artificial Intelligence (AI) Act[288]

In April 2021, the European Commission adopted a proposal in the draft AI Act [289] that sets out a harmonised legal framework for the development, supply, and use of AI products and services in the EU but which also addresses the potential harms. The framework preamble specifically acknowledges that when AI technologies are used in “real-time” for identification purposes they risk the fundamental rights of people. [290] The proposed legal framework is aimed at regulating AI systems through a ‘risk based' classification system and lays down different legal obligations.[291] In contrast to the UK Bill, the draft act currently proposes to ban the use of AI systems for the “live” remote biometric identification of persons in publicly accessible spaces for the purpose of law enforcement. [292] However, this ban is qualified and subject to exceptions where the risks to data protection are outweighed by a substantial public interest.[293] The exceptions included at Article 5(1)(d) vary in scope and are; (i)“targeted searches for potential victims of crime and missing children”, (ii) “prevention of specific, substantial and imminent threat to life or physical safety of persons or a terrorist attack” and (iii) “detection, localisation, identification or prosecution of a perpetrator or individual suspected of a criminal offence” referred to in the European Arrest Warrant

[288] Supra 22

[289] Ibid.

[290] Ibid. p 3

[292] Supra 22 art 5(1)(d) recital 33 and annex III(1)(a).

[293] Supra 22 art 5(1)(d)

Framework Decision.[294] It is acknowledged that the general ban may restrict arbitrary live FRT deployments by law enforcement and the risks to data protection and privacy with minor criminal activity or with public protesting.[295] Law enforcement relying on the exceptions to deploy Live FRT deployments would however still be subject to the legal principles enshrined in the LED and the GDPR. Recital 21 and Article 5(3) of the proposed framework stipulates the use shall be subject to 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".[296] Overall, the introduction the AI Act may increase the complexity of the LED and GDPR and the importance of the data protection authority in Member States in ensuring that the exceptions are robustly and tightly enforced.

In response to the draft framework, the EDPS and EDPB have raised concerns and jointly advocate a general ban on *any* AI use for the automated recognition of human features in publicly accessible spaces, including faces "in any context".[297] They maintain that biometric identification presents a "high risk of intrusion" into peoples' private lives.[298] The use of AI systems with live FRTs also presents serious proportionality problems [299] because it involves and impacts an "indiscriminate and

[294] Ibid.

[295] Theodore Christakis and Mathias 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/ (accessed 26 May 2023).

[296] Supra 22 art 5(3) rec 21

[297] 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) 3 https://edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf (accessed 24 May 2023).

[298] Ibid. p 2-3.

[299] Ibid. p 13

disproportionate number of data subjects for the identification of very few people".[300] This view is certainly supported in the deployment statistics and results reported by the MPS and SWP in the UK and previously discussed above. Furthermore, they contend that proposed exceptions in the Act are deficient because of insufficient solutions to correctly notify people about biometric processing [301] and to safeguard the timely and effective use data protection rights.[302] These criticisms are especially relevant and applicable to the current practice of FRT deployments by law enforcement in the UK. The criticisms underline the serious challenges faced by law enforcement in achieving lawful live FRT deployments and demonstrating fully compliance with all data protection and privacy laws.

Although the agreed version of the framework is yet to be finalised before it becomes law, the proposed framework has also proven controversial with the European Parliament which made several significant amendments. It is clear from the June 2023 Parliamentary plenary[303] that there is majority Parliamentary support for a ban on the use of live as well as ex-post use biometric identification systems which would include live FRTs. The only exception for live system use would be restricted to cases of "severe crime".[304] Furthermore, Parliament is seeking a ban on all biometric categorisation systems relying on sensitive characteristics (e.g. gender, race, ethnicity); predictive policing systems (e.g. profiling, or past criminal behaviour); and AI systems using indiscriminate scraping of biometric data from CCTV footage to

---

[300] Ibid. p 30

[301] Ibid. p 12

[302] Ibid.

[303]European Parliament Plenary 'Parliament's negotiating position on the artificial intelligence act' (2023) 2 https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/747926/EPRS_ATA(2023)747926_EN.pdf (accessed 20 June 2023)

[304] Ibid.

create databases or watchlists. The effect of these bans will be to eliminate or reduce the potential harms of these AI based systems.

It is clear from a consideration of the proposed changes in the UK Bill and the EU draft AI Act that there are significant differences in the approach to the regulation of live FRTs. The different landscapes that are likely to emerge will have a differential effect on the deployment of live FRTs by law enforcement in the two jurisdictions. The landscape to emerge in the UK may be dominated by a more permissive data protection framework that promotes the normalisation of live FRT deployments by law enforcement while that in the EU is likely be more restrictive. Compared to the approach in the UK, the EU changes may be more likely to better control and regulate the proliferation of live FRT deployments by law enforcement and better control the harms and risks to data protection and privacy rights enshrined in the data protection frameworks.

CONCLUSION

It is important for UK law enforcement to avail of advanced technologies available in the fight against crime and for maintaining public safety. Understandably, LEAs need to be equipped to identify terror suspects and perpetrators of the most serious crimes quickly and efficiently. FRTs may be part of the solution to accomplish this but do not provide a "silver bullet".[305] Live FRT deployments have become a more frequent reality that create significant risks to data protection and privacy and harmful to both in a democratic society. The risks and harms that are generated vastly outweigh the potential benefits that are claimed in support but have not yet materialised. It is difficult to conclude that live FRT deployments can be *fully* compatible with the data protection legal framework and do not interfere with the individuals Article 8 ECHR. Neither is it possible at this stage to be completely satisfied that deployments can potentially occupy a legitimate place within these legal frameworks. Compliance with some Part 3 DPA 2018 requirements are achievable, but significant and legitimate concerns remain around the legal basis of deployments that must be addressed.

The validity of judgments made by law enforcement about deployments being "strictly necessary" and satisfying the principle of "proportionality" are seriously undermined by current reliance on broad deployment purposes. They are also undermined and appear flawed when the poor outcomes (alert levels) reported are weighed against the large scale, indiscriminate, and disproportionate interference with, and sacrifice of data protection and Article 8 ECHR. Demonstrating full compliance with the full range of data protection principles and demonstrating the technology is built with protection by design has not yet been fully achieved. This problem is compounded by the claims of developers about FRTs trade secrets and intellectual property rights.[306] The software limitations in systems and the AI technology uncertainties further evidence why the technology and deployments lack functional certainty and cannot be treated as fully compliant with key data principles or be legally compatible.

[305] Supra 27 p 27

[306] Ibid.

The UK Bill to amend the data protection laws fails to offer an effective solution to better regulate live FRT use by law enforcement. It may accelerate the “normalisation” of deployments and reduce the obligations on law enforcement. The Bill may produce a “permissive regime” and cause further harms to data protection and privacy. It may also jeopardise the “equivalent level of protection” currently enjoyed with the EU and bring other consequences. The draft AI Act may restrict live FRT deployments by law enforcement in the EU to limited circumstances around serious crimes. This development would go some way to stricter control of live FRT use and lead to a “restrictive regime” but a more complex data protection legal framework. Regardless of the landscape that emerges in the two jurisdictions, Article 8 ECHR remains important in safeguarding data protection and privacy rights, and in challenging whether deployments are necessary in a democratic society.

A ban on live FRTs would eliminate the risks and harms they create. In the absence of the same, compatibility may be *improved* with more robust enforcement by the ICO. Stricter regulation and enforcement are needed through a separate legal framework including; (i) more focused safeguards, (ii) stricter obligations on “strictly necessary” and “proportionality” assessments, (iii) limiting discretion, and (iv) broadening assessments to include bias and discrimination. These provisions would better ensure that all the risks created by the use or deployment of live FRTs are properly weighed and balanced and more valid and objective judgements are achieved. Perhaps then it may be more realistic to conclude that compatibility *can* be achieved and the power asymmetries emerging between those deploying and those impacted can be tackled.

BIBLIOGRAPHY

Ahmad W and Dethy E, 'Preventing surveillance cities: Developing a set of fundamental privacy provisions' (2019) Journal of Science Policy & Governance, 15(1) 1 https://www.sciencepolicyjournal.org/uploads/5/4/3/4/5434385/ahmad_dethy_jspg_v15.pdf (accessed 25 May 2023).

Antrag auf Zulassung der Berufung §§ 124, 124a VwGO, Hamburg DPA, 13 March 2020, https://datenschutz-hamburg.de/assets/pdf/Antrag_Zulassung_Berufung_2020-03-13.pdf (accessed 18 June 2023).

Aycaguer v. France no. 8806/12 ECHR, 2017-V https://hudoc.echr.coe.int/eng?i=001-174441 (assessed May 2023).

Bambauer J, 'Facial recognition as a less bad option' (2021) Aegis Series Paper No. 2107. https://www.hoover.org/sites/default/files/research/docs/bambauer_webreadypdf.pdf (accessed on 2 May 2023).

Bank Mellat v HM Treasury (No 2) [2013] UKSC 39 https://www.supremecourt.uk/cases/docs/uksc-2011-0040-judgment.pdf (accessed 18 June 2023)

Big Brother Watch Briefing on the Data Protection and Digital Information 2.0 Bill for House of Commons Committee Stage (2023) https://bigbrotherwatch.org.uk/wp-content/uploads/2023/05/Big-Brother-Watch-Briefing-on-the-Data-Protection-and-Digital-Information-2.0-Bill-for-House-of-Commons-Committee-Stage.pdf (accessed 5 June 2023).

Bowling B and Iyer S, 'Automated policing: The case of body-worn video' (2019) International Journal of Law in Context, 15(2), 140 https://doi.org/10.1017/S1744552319000089 (accessed 25 May 2023).

Buolamwini J et al., 'Facial Recognition Technologies: A Primer' (2020) https://people.cs.umass.edu/~elm/papers/FRTprimer.pdf (accessed 1 June 2023).

C-275/06 *Productores de Música de España (Promusicae) v. Telefónica de España SAU* [2007] ECR I-274, Opinion of AG Kokott, para. 53 https://curia.europa.eu/juris/document/document.jsf?text=&docid=62901&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1188483 (accessed 29 April 2023).

C-434/16 *Peter Nowak v Data Protection Commissioner* [2017] ECR 994, para. 53 https://curia.europa.eu/juris/document/document.jsf?text=&docid=198059&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1163161 (accessed 30 June 2023).

C-698/15 *Tele 2 Sverige*, [2016] ECR 970, para 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 (accessed 18 June 2023).

Centre for Data Ethics and Innovation 'Snapshot Paper - Facial Recognition Technology' (2020) https://www.gov.uk/government/publications/cdei-publishes-briefing-paper-on-facial-recognition-technology/snapshot-paper-facial-recognition-technology (accessed 2 May 2023).

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/ (accessed 26 May 2023).

Commission Implementing Decision pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom 2021, https://commission.europa.eu/system/files/2021-06/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_law_enforcement_directive_en.pdf (accessed on 29 May 2023).

Commission Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, 2021, https://commission.europa.eu/system/files/202106/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf (accessed on 29 May 2023).

Commission Nationale de l'Informatique et des Libertés (CNIL) 'Reconnaissance faciale - Pour un debat à la hauteur des enjeux' (2019) https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-lahauteur-des-enjeux (accessed 27 May 2023).

Copland v United Kingdom, no. 62617/00, ECHR 2007- IV https://hudoc.echr.coe.int/eng?i=001-79996 (accessed 26 June 2023).

Council of Europe, 'Guidelines on Facial Recognition', (2021), https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3 (accessed 20 March 2023).

Data Protection and Digital Information (No. 2) HC Bill (2022-23) [314] https://bills.parliament.uk/bills/3430 (accessed 26 June 2023).

Data Protection and Digital Information (No. 2) Bill: European Convention on Human Rights Memorandum (8 March 2023) https://publications.parliament.uk/pa/bills/cbill/58- 03/0265/echrmemo.pdf (accessed 5 June 2023).

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 (accessed 28 June 2023).

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 (accessed 28 June 2023).

Demetzou K, 'Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation' (2019) Computer Law & Security Review, 35(6), 105342 https://doi.org/10.1016/j.clsr.2019.105342 (accessed 12 May 2023).

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] L 119/89 (The Law Enforcement Directive or LED). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG (accessed 1 April 2023).

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) 3 https://edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf (accessed 24 May 2023).

European Commission ‘Data protection: Commission adopts adequacy decisions for the UK Brussels’, 28 June 2021 https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_21_3183/IP_21_3183_EN.pdf (accessed 4 January 2023).

European Convention of Human Rights (ECHRs) https://www.echr.coe.int/Documents/Convention_ENG.pdf (accessed 4 January 2023).

European Data Protection Board Guidelines 3/2019 on processing of personal data through video devices – version for public consultation (2019) 30-31 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf (accessed 24 June 2023).

European Data Protection Board Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement (26 April 2023) **(**Version 2.0) https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf (accessed 27 May 2023).

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 (accessed 23 January 2023).

European Parliament Plenary ‘Parliament's negotiating position on the artificial intelligence act’ (2023) https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/747926/EPRS_ATA(2023)747926_EN.pdf (accessed 20 June 2023)

European Union Agency for Fundamental Rights, ‘Data quality and artificial intelligence - mitigating bias and error to protect fundamental rights’, (2019) https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf (accessed 20 March 2023).

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 (accessed 20 May 2023).

European Union Agency for Fundamental Rights, ‘Under watchful eye -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 (accessed 15 January 2023).

Face Me Team ‘How Facial Recognition Enhances Smart Banking’ (2022) https://www.cyberlink.com/faceme/insights/articles/599/facial-recognition-for-smart-banking (accessed 3 June 2023).

Fagan J et al, 'Stops and stares: Street stops, surveillance, and race in the new policing' (2016) Fordham Urban Law Journal Vol 43, 14 https://ssrn.com/abstract=2758852 (accessed 3 May 2023).

Gaughran v Chief Constable of Northern Ireland, no. 45245/15 ECHR 2020-I https://hudoc.echr.coe.int/eng?i=001-200817 (accessed 3 July 2023).

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 (accessed 20 February 2023).

Impact Assessment Data Protection and Digital Information (No. 2) Bill: European Convention on Human Rights Memorandum https://www.gov.uk/government/publications/data-protection-and-digital-information-bill-impact-assessments/data-protection-and-digital-information-no-2-bill-european-convention-on-human-rights-memorandum (accessed 5 June 2023).

Information Commissioner's Annual Report and Financial Statements 2019-2020, https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83- certified.pdf (accessed on 3 June 2023)

Information Commissioner's Opinion 'The use of live facial recognition technology by law enforcement in public places' (2019) https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf (accessed on 12 May 2023).

Information Commissioners Office (ICO) Guide to the UK General Data Protection Regulation (UK GDPR) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ (accessed on 29 April 2023).

Information Commissioner's Response to the Data Protection and Digital Information (No 2) Bill (DPDI No 2 Bill) (2023) https://ico.org.uk/media/about-the-ico/consultation-responses/4025316/response-to-dpdi-bill-20230530.pdf (accessed 5 June 2023).

Italian Data Protection Authority. Parere sul sistema Sari Real Time (2021) https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575877 (accessed 23 July 2023).

Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Others* [2014] ECR 238 https://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1419450 (accessed 18 June 2023).

Kak A, 'Regulating Biometrics: Global Approaches and Urgent Questions' AI Now Institute, (2020) https://ainowinstitute.org/regulatingbiometrics.html (accessed 3 January 2023).

Kindt E, ‘Having yes, using no? About the new legal regime for biometric data’ (2018) Computer law & security review. Jun 1;34(3): 523 https://doi.org/10.1016/j.clsr.2017.11.004 (accessed 20 May 2023).

Leslie D, ‘Understanding bias in facial recognition technologies’ (2020) https://zenodo.org/record/4050457/files/Understanding%20bias%20in%20FRT%20FINAL.pdf?download=[1] (accessed 25 May 2023).

Mclaughlin M and Castro ‘The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist’ (2020) Available at: https://itif.org/sites/default/files/2020-best-facial recognition.pdf (accessed on 17 May 2023).

Metropolitan Police Service Appropriate Policy Document for sensitive data processing within Live Facial Recognition deployments (2023) https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/new/mps-lfr-apd---v.2.0-web.pdf (accessed 17 June 2023).

Metropolitan Police Service LFR deployments (2023) https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/new/lfr-deployment-grid.pdf (accessed 17 July 2023).

Metropolitan Police Service LFR Policy Document Direction for the MPS Deployment of overt Live Facial Recognition Technology to locate person(s) on a Watchlist (2023) https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/policy-documents/lfr-policy-document2.pdf (accessed 17 June 2023).

M.K. v France, no.19522/09, ECHR 2013-V https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-119075&filename=001-119075.pdf (accessed 23 June 2023).

Mobilio G, ‘Your face is not new to me–Regulating the surveillance power of facial recognition technologies’. (2023) Internet Policy Review, 12(1) 2 https://doi.org/10.14763/2023.1.1699 (accessed on 29 April 2023).

Osoba O & Welser IV W, ‘An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence’ (2017) RAND Corporation, RR-1744-RC. https://www.rand.org/pubs/research_reports/RR1744.html (accessed 27 March 2023).

Pounder C, ‘Facial recognition CCTV excluded from new data protection law by definition of “personal data”’ (2023) https://amberhawk.typepad.com/amberhawk/2023/04/facialrecognition-cctv-excluded-from-new-data-protection-law-by-definition-of-personal-data.html (accessed 5 June 2023).

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), Article 5(1)(d) and recital 33 and annex III(1)(a) https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF (accessed 25 July 2023).

Raposo VL, ‘When facial recognition does not ‘recognise: erroneous identifications and resulting liabilities’ (2023) AI & Society https://doi.org/10.1007/s00146-023-01634-z (accessed 17 May 2023).

R (on the application of Edward Bridges) v The Chief Constable of South Wales Police and others [2019] EWHC 2341 https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf (accessed 27 May 2023).

R (on the application of Edward Bridges) v The Chief Constable of South Wales Police [2020] EWCA Civ 1058 https://www.bailii.org/ew/cases/EWCA/Civ/2020/1058.html (accessed 20 May 2023).

R (Catt) v Association of Chief Police Officers [2015] UKSC 9, [2015] AC 1065 at [7] https://www.supremecourt.uk/cases/docs/uksc-2013-0112-judgment.pdf (accessed 10 May 2023).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation (GDPR)) [2016] OJ L119/1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 (accessed 1 April 2023).

Roussi A, 'Resisting the rise of facial recognition', 350 https://www.nature.com/articles/d41586-020-03188-2 (accessed 2 May 2023).

Ryder M, 'Independent legal review of the governance of biometric data in England and Wales' (2022) https://www.adalovelaceinstitute.org/wp-content/uploads/2022/06/The-Ryder-Review-Independent-legal-review-of-the-governance-of-biometric-data-in-England-and-Wales-Ada-Lovelace-Institute-June-2022.pdf (accessed 25 May 2023).

S and Marper v United Kingdom, nos. 30562/04 and 30566/04 [2008] ECHR https://hudoc.echr.coe.int/eng?i=001-90051 (accessed 20 July 2023).

Selinger E and Hartzog Woodrow, 'The Case for Banning Law Enforcement from using Facial Recognition Technology' (2020) https://theappeal.org/wp-content/uploads/2020/12/20.08_Facial-Recognition-1.pdf (accessed 20 May 2023).

South Wales Police Data Protection Impact Assessment (DPIA) (2022) https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/live-facial-recognition/live-frt-docs-july-23/lfr-dpia-v0.7.pdf (accessed 17 July 2023).

South Wales Police 'Law enforcement processing: Part 3 Appropriate Policy Document' https://www.southwales.police.uk/SysSiteAssets/media/downloads/south-

wales/policies-and-procedures/part_3_appropriate_policy_document.pdf (accessed 17 June 2023).

South Wales Police LFR Deployments (2023) https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/live-facial-recognition/all-lfr-deployments-lleoliadau-up-to-2-july-2023.pdf (accessed 17 July 2023).

Sporrong and Lönnroth v Sweden (1982) 5 EHRR 35, para 69.

Thales, 'Biometrics: definition, use cases, latest news' (2021) https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics (accessed on 19 Feb 2023).

UK General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council (UK GDPR).

Yeung D et al., 'Face Recognition Technologies: Designing Systems that Protect Privacy and Prevent Bias' (2020) ix-x https://www.rand.org/content/dam/rand/pubs/research_reports/RR4200/RR4226/RAND_RR4226.pdf (accessed 20 May 2023).