IN THE HIGH COURT OF JUSTICE **Claim no. ACN-2024-LON-001764**
KING'S BENCH DIVISION (ADMINISTRATIVE COURT)
BETWEEN:

THE KING (on the application of)
(1) SHAUN THOMPSON
(2) SILKIE CARLO

Claimants

-and-

THE COMMISSIONER OF POLICE OF THE METROPOLIS

Defendant

-and-

THE EQUALITY AND HUMAN RIGHTS COMMISSION

Intervener

SKELETON ARGUMENT ON BEHALF OF THE CLAIMANTS
For the substantive hearing on 27-28 January 2026

References: Core Bundle [CB/pg]; Supplemental Bundle [SB/pg]; Amended Statement of Facts and Grounds (SFG/para); Detailed Grounds of Defence (DGD/para); submissions of the EHRC (EHRC/para); witness statements/expert reports (surname-statement/report number/para).

A. INTRODUCTION

1. This claim concerns the Metropolitan Police Service's ('**MPS**') use of live facial recognition ('**LFR**') technology to locate persons of interest in public places in London. LFR is an artificial intelligence-driven technology which works by scanning the faces of anyone passing a CCTV camera linked to an LFR system, extracting unique biometrics and comparing them to those of people on a "watchlist" of persons the police are seeking to locate. All of this is done automatically, near instantaneously and involves vast numbers of people. The MPS' use of LFR, and the technology's capacity, are expanding rapidly. Watchlists routinely include over 15,000 people and, this year alone, the MPS has deployed LFR on more than 200 occasions, during which an estimated 3.5m million faces have been captured and their unique facial biometrics processed.

2. LFR is undoubtedly a very powerful tool, and its development of enormous significance for law enforcement. The MPS describes LFR as "*game-changing*" one of the "*biggest breakthroughs…since the discovery of DNA"* (Chiswick 2/33) [CB/328] and as "*revolutionising*" policing [SB/43]. It is also precisely

because of its "*raw power*", however, that, as the courts have recognised, LFR raises "*significant civil liberties concerns*" which mean it is critical that there are sufficient safeguards to protect against "*the potential baleful uses to which [LFR] could be put by agents of the state and others*" (*R (Bridges) v Chief Constable of South Wales Police* [2020] 1 WLR 672 ('***Bridges DC***') §7). In a similar vein, the European Court of Human Rights ('**ECtHR**') has described LFR as "*highly intrusive*" (*Glukhin v Russia* (2024) 78 EHRR 6 §90) and noted that "*it is essential in the context of implementing facial recognition technology to have detailed rules governing the scope and application of measures, as well as strong safeguards against the risk of abuse and arbitrariness. The need for safeguards will be all the greater where the use of live facial recognition technology is concerned*" (§82).

3. In the first test case concerning police use of LFR, the Court of Appeal ("**CA**") in *Bridges* [2020] 1 WLR 5037 ('***Bridges CA***'), disagreeing with the DC, found that South Wales Police's ('**SWP**') use of LFR was not accompanied by sufficient safeguards to ensure its use was in accordance with the law ('**IAWL**') for the purpose of Article 8 of the European Convention on Human Rights ('**ECHR**'). In particular, there were insufficient constraints on police discretion as to "*where*" LFR could be used and "*who*" could be placed on an LFR watchlist. That meant that "*too much discretion [was] left to individual police officers" (Bridges CA* §91). The question in the present case is whether that is also true of the MPS' use of LFR in relation to the "*where*" question. Do MPS officers have "*too much discretion*" as to "*where*" LFR can be deployed such that interferences with the rights protected by Article 8 (Ground 1), as well as Articles 10 and 11 ECHR, are not IAWL/prescribed by law ('**PBL**') (Ground 2).[1] That is an issue of real importance. If where LFR can be used is not sufficiently constrained, such that people's identities can be constantly checked in any public place at any time to see if they are of interest to the police, that would transform public spaces and how society is policed.

B. THE CLAIMANTS

4. The first Claimant, Mr Thompson, was born and lives in London. He volunteers with children and young people affected by youth violence to prevent them from

[1] In the Amended SFG these are Grounds 3 and 4 but Grounds 1 and 2 (which related to the MPS' use of LFR under a policy framework which it has now replaced) were withdrawn by consent [CB/168].

coming into contact with the criminal justice system (Thompson 1/6) [CB/281]. On 23 February 2023, he was stopped, detained, and questioned by MPS officers near London Bridge station upon being falsely identified by LFR as an individual on a watchlist. Although the officers did not consider Mr Thompson to be the individual he was flagged as being, they still scrutinised his facial features and pressed him to provide his fingerprints through a mobile scanner. He ultimately had to produce his passport to prove his identity (Thompson1/27-30) [CB/284]. The second Claimant, Ms Carlo, is the director of the civil-liberties organisation, Big Brother Watch. She also lives in London, and has monitored the MPS' use of LFR since its inception including by attending LFR deployments. Ms Carlo often attends/organises protests and is concerned about the prospect of LFR being used at such events.

C. PROCEDURAL HISTORY

C1. Background to the challenge under consideration

5. This claim was issued on 24 May 2024 challenging both the "*where*" and the "*who*" elements of the policy then in place. It was accompanied an expert report from Martin Utley, a Professor of Operational Research at University College London, which showed that the Defendant's then applicable policy, which purported to limit where LFR could be deployed, in fact enabled deployment across large areas of London. The Defendant immediately announced a review of its LFR policy, pending which the claim was stayed.

6. The current policy was published on 11 September 2024, significantly revising the previous framework: all the "*who*" aspects of the previous policy about which the Claimants had complained were removed, and a new approach to the "*where*" question was adopted. In October 2024, the Claimants amended their claim to challenge the MPS' use of LFR under the Policy.[2] Farbey J granted permission to apply for judicial review on 30 May 2025 [CB/165] and the EHRC was granted permission to intervene by an order dated 2 July 2025 [CB/171].

C2. Applications to rely on evidence

[2] The parties subsequently compromised the claim as it related the use of LFR under the policy in place at the time Mr Thompson was stopped and when the claim was issued. The Defendant agreed to pay Mr Thompson a substantial settlement sum and the Claimants' costs of that aspect of the claim [CB/168]).

7. When filing the amended grounds, the Claimants applied to rely on a second expert report from Prof Utley, dated 8 October 2024 [CB/371]. That report provides mathematical analysis of criteria contained in the Policy regarding where LFR technology can be deployed. On 16 September 2025, Farbey J granted permission to rely on that report "*de bene esse*" [CB/173]. On 21 November 2025, the Claimants applied to rely on a supplemental expert report from Prof Utley [CB/406]. It responds to mischaracterisations of Prof Utley's second report in the DGD and Ms Chiswick's statement, served on 10 October 2025. It also deals with further information provided by Ms Chiswick and in a subsequent letter from the MPS. The Claimants also applied on 21 November 2025 to rely on a further witness statement from Ms Carlo which responds to factual points made by Ms Chiswick. The Court is respectfully invited to consider this evidence on the same *de bene esse* basis as Prof Utley's second report and Ms Carlo's third witness statement.

D. LFR TECHNOLOGY AND THE MPS' USE OF IT

8. LFR is a biometric technology, meaning it quantifies a person's physical and physiological characteristics, known as biometric data, which allows for their unique identification.[3] Other forms of biometric technology include fingerprinting, DNA profiling, gait analysis, and iris scanning. There is no dispute about how the LFR technology used by the MPS works. While the technology is constantly changing and improving its basic functioning is the same as that considered by the courts in *Bridges* (see *Bridges CA* §9; Chiswick 2/4) [CB/321]. In short, the system captures the facial biometrics of each person passing CCTV cameras and compares them to those of every person on a watchlist. If it assesses two sets of facial biometrics to be sufficiently similar, it generates a positive match, officers are alerted and may then intervene to seek to ascertain whether the person whose face has been captured - in real time - is a person they are seeking.

9. The MPS first used LFR in 2016 to monitor those attending the Notting Hill Carnival. LFR was used on just nine occasions between 2020, and 2022 and only 19 times in 2023. There has since been a dramatic increase: LFR was deployed on 180 occasions in 2024 and 201 in the year to date. While the number of deployments is up by 12% in 2025, there has been 280% increase (as

[3] European Data Protection Board, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement* (v 2.0) (April 2023) §7. [SB/68]

compared to 2024) in the number of faces whose unique biometrics the MPS has captured and processed.[4] Amidst this escalation in use and in the number of people whose rights are affected, the way in which the MPS is using LFR is changing. Earlier this year, the MPS announced that the first permanent facial recognition cameras would be installed on buildings and lampposts in Croydon (Carlo 5/6) [CB/313]. While Ms Chiswick suggests a number of practical limitations to integrating LFR into London's extensive existing CCTV networks, she does not identify any principled basis why such use is not permitted under the MPS' policy framework (Chiswick 2/11) [CB/322].

E. THE MPS' LFR POLICY

10. There is no bespoke statutory regime governing the use of LFR by the police. Rather, LFR is deployed under the MPS' general common law powers to obtain and store information for policing purposes (*Bridges CA* §38). The MPS has a published Policy which governs officers' use LFR. The Policy deals with "*where*" LFR can be deployed by reference to three "use cases". "Use Case A" permits deployment at "*hotspots*"; Use Case B permits deployment to support "*protective security operations*" ("**PSOs**"); Use Case C permits deployment where there is "*specific intelligence concerning the likely location [of] … "sought persons"*.

E1. USE CASE A

11. Use Case A concerns "*crime hotspots*" and "*missing persons hotspots*". The first is defined as follows:

> *2.3 A crime hotspot is a small geographical area of approximately 300-500m across where crime data and/or MPS intelligence reporting and/or operational experience as to future criminality indicates that that it is an area where:*
> *(i) the crime rate; and/or*
> *(ii) the rate at which crime in that area is rising,*
> *is assessed to be in the upper quartile for that BCU/OCU area* [CB/186].

12. A BCU is a geographic "*Basic Command Unit*" and London is divided into 12 BCUs. An "OCU" is an "*Operational Command Unit*", which is not a geographic area in and of itself. It has emerged in evidence that an "*OCU area*" relates to places that OCUs police, e.g. royal residences, Heathrow and City airports and the parliamentary estate (Chiswick 2/51) [CB/333]

[4] These numbers are taken from the Defendant's live LFR deployment records as at 5 December 2025.

13. A "*missing person's hotspot*" is a 300-500m area where "*intelligence reporting and/or operational experience indicates missing persons are likely to be present*" (Policy §2.3(b)) [CB/186].

14. Under Use Case A, LFR can be used "*at the hotspot*" (i.e. within the 300-500m geographical area) and "*at access routes within an approximately 300m radius of a hotspot location*" (Policy §5.2) [CB/191]. The meaning of "*access routes"* is set out further below.

E2. USE CASE B

15. Use Case B provides that LFR may be used to "*support*" two categories of PSO (§2.7):

> *(a) a PSO which has as its objective the protection of critical national infrastructure (a "CNI PSO");*
>
> *(b) a PSO undertaken by the MPS in respect of events which are expected to attract public attendance and, further, where the MPS has intelligence which indicates that there is likely to be a threat to public safety (an "Event PSO")* [CB/186].

16. As to a CNI PSO, LFR can also be used "*within and up to an approximate 300m radius of the external boundary area of the critical national infrastructure or event … or at the nearest practicable location to the nearest operational transport access points to the critical national infrastructure or event*" (Policy §5.3) [CB/191]. CNI is not defined in the Policy. The Defendant has stated in evidence that the MPS applies the broad National Protective Security Authority definition of CNI as "*critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in: a) Major detrimental impact on the availability, integrity or delivery of essential services and/or "(b) Significant impact on national security, national defence, or the functioning of the state"* (Chiswick 2/117) [CB/350].

E3. USE CASE C

17. Pursuant to Use Case C, LFR can be used at "*a particular location where the [Met] has concluded, based on specific intelligence, that a person who is eligible for inclusion on a LFR Watchlist…is likely to be at that location"* (Policy §2.9) [CB/187]. While the "*purpose*" of a deployment undertaken pursuant to

this use case is said to be "*locating the relevant watch listed person*", the watchlist must include a large number of other individuals, given the Policy provides that various categories of individuals "*will be*" added to the watchlist where intelligence indicates that "*a person*" falling within those categories is likely to be in the area. Thus, the Policy mandate that where *one* person in any watchlist category is likely to be at the relevant location, *every* person from all the watchlist categories will automatically be added to the watchlist, even if they have no connection to the specific intelligence, location and the original purpose of deployment.

F. LEGAL PRINCIPLES

F1. THE IN ACCORDANCE WITH THE LAW/PRESCRIBED BY LAW REQUIREMENT

18. An interference with the qualified rights protected by Article 8, 10 and 11 ECHR will breach the right in question unless it is IAWL (Article 8) or PBL (Articles 10 and 11). It must also pursue one of the legitimate aims set out in these Articles and be necessary in a democratic society. This case is concerned with the first of these conditions of lawful interference: the IAWL/PBL[5] requirement, which the case law sometimes refers to as the "*test of legality*".

19. The case law breaks down the IAWL requirement into four broad sub-requirements; it is the third and fourth of these requirements which are at issue in this case.

    19.1. A measure or power that interferes with the right must have a basis in domestic law and there must, as a minimum, be compliance with that law.

    19.2. The legal basis/law regulating the measure must be adequately accessible.

    19.3. The law must be sufficiently "*foreseeable*" as to the circumstances in which and conditions on which a public authority is entitled to resort to the measure which affects rights (*Martínez v Spain* [GC] (2015) 60 EHRR 3 §117). Put another way, the law must indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authority (e.g. *Rotaru v Romania* [GC] (2000) 8 BHRC 449 §60; *Versaci v* Italy, App No. 3795/22, 15 May 2025 §112).

[5] These expressions bear the same meaning. The shorthand "IAWL" is used to refer to both.

19.4. Closely related is the requirement that the law must be "*compatible with the rule of law*," which means that there must be adequate safeguards in domestic law against arbitrary and/or disproportionate interferences with Convention rights by public authorities (*Magyar Kétfarkú Kutya Párt v Hungary* [GC] (2020) 49 BHRC 411 §93. See also, *Beghal v DPP* [2016] AC 88 §32). Those "safeguards" constrain wide discretionary powers and ensure that the application of a measure is foreseeable (see e.g. *Gillan v UK* (2010) 50 EHRR 45 §79; *AR v UK,* App No. 6033/19, 1 July 2025 §61, 64; *Re Gallagher* §24).

20. The courts have on many occasions considered whether discretionary powers satisfy the third and fourth requirements. An important part of this assessment is whether measures are "*sufficiently curtailed*" or "*sufficiently circumscribed*" (e.g. *Beghal v UK* (2019) 69 EHRR 28 § 89, 109; *Gillan* §87). Where public authorities are left with an "*excessively broad discretion*" (e.g. *AR v UK,* App No. 6033/19, 1 July 2025 §68; *Gillan* §83-85; *Re Gallagher* §31) or a discretionary power affords them "*too much latitude*" (e.g. *Domenichini v Italy* (2001) 32 EHRR 4 §32) the relevant measure will not be IAWL.

21. Whether safeguards and constraints are sufficient to ensure exercise of powers are IAWL depends on, among other things, the nature of a power, the extent to which it intrudes with Convention rights, the field, and the number of people affected by its use (e.g. *AR* § 60; *Beghal v UK* §92; *Bridges CA* §82, 87). The ECtHR has stressed that the development of powerful surveillance technologies involving the processing of personal data has increased the need for robust safeguards constraining the exercise of discretionary powers (e.g. *Szabo & Vissy v Hungary* (2016) 63 EHRR 3 §68; *Catt v UK* (2019) 69 EHRR 7 §114).

F2. THE *BRIDGES* CASE

22. The *Bridges* case was the first to consider the use of LFR by police.[6] Mr Bridges challenged two deployments of LFR by SWP in December 2017 and March 2018, as well as the force's ongoing use of LFR, which involved watchlists of 400-800 people, with a contractual limit of 2000 (*Bridges DC* §31). Mr Bridges argued

[6] The label AFR (Automated Facial Recognition) was used in that case, with AFR Locate being the name for the software, but it is understood to be common ground that the systems are substantially the same.

that the use of LFR was not IAWL for the purposes of Article 8 ECHR (the other grounds of challenge are not relevant for present purposes).

23. At the material time, SWP deployed LFR pursuant to a multi-layered legal framework, which is summarised in *Bridges DC* at §22 and Annex A. That is important for present purposes as the Defendant here relies on a series of similar features. The applicable framework in *Bridges* included requirements or stipulations in SWP's published Standard Operating Procedures that: (a) watchlists must be proportionate and necessary; (b) pre-deployment reports have to set the rationale for using LFR; (c) the use of signage to advertise deployments, making individuals aware LFR is in use before their image is captured; (d) that LFR deployment are authorised at a certain level (by silver commanders); and (e) interventions must be based on officers establishing identity using traditional policing methods (i.e. the human in the loop). That policy sat below the statutory requirements of the Data Protection Act 2018, the Surveillance Camera Code of Practice and guidance which remain in place today.

24. The DC and CA applied the well-established principles (discussed above) concerning the IAWL requirement (*Bridges DC* §80; *Bridges CA* §55). The DC concluded that there was a "*clear and sufficient legal framework governing whether, when and how [LFR] may be used*" (§84, see also §96). The DC considered the following aspects of that framework to be of significance: (a) the requirements of data protection law that processing be strictly necessary for law enforcement purposes and that it also be necessary for one more of the purposes set out in Sch 8 to the DPA 2018 (§87); (b) provisions of the Surveillance Camera Code of Practice (to which chief officers must have regard) concerning, inter alia, when and where cameras should be used and the requirement that adverse action should not be taken without human intervention, as well as the bespoke provisions on the requirement for the use of LFR systems to be proportionate, which the DC emphasised in setting out the legal framework in the annex to its decision (§90 and Annex A); (c) SWP's standard operating procedures, including requirements that deployments be overt, CCTV imagery be retained for a maximum period, and guidelines on the responsibilities of officers operating the system, including where there is a positive match (§93); and (d) deployment reports requiring officers to specify in advance the purposes and justification for a deployment (§94).

25. The CA disagreed with the DC's conclusion that the framework was sufficient to ensure that SWP's use of LFR was IAWL (*Bridges CA* §90). That was because it did not "*sufficiently set out the terms on which discretionary powers [to use LFR could] be exercised by the police*" (§94). Specifically, the "*critical defects*" were that "*too much discretion"* was left to officers in respect of who could be placed on a watchlist (what the CA called the "who question") and where it could be deployed (the "*where*" question) (§91).

26. On the "who" question, the CA noted that SWP could place people on watchlists if they were "*wanted on suspicion for an offence, wanted on warrant, vulnerable persons and other persons where intelligence is required*" (§123). That was not sufficient because the last of these categories left "*too broad a discretion vested in the individual police officer to decide who should go onto the watchlist*" (§124). On the "*where*" question, the CA held that "*it will often, perhaps always, be the case that the location will be determined by whether the police have reason to believe that people on the watchlist are going to be at that location*" (§96). The "*question of the location [is left] to the discretion of individual police officers*" (§130). This was insufficient to meet the IAWL requirement. The CA noted specifically that "*[it was] not said, for example, that the location must be one at which it is thought on reasonable grounds that people on the watchlist will be present*" (§130).

G. THE "CIVIL LIBERTIES" CONCERNS ABOUT LFR AND THE REASONS UNDERLYING THE "WHO" AND "WHERE" REQUIREMENTS

27. As noted above, the domestic courts and the ECtHR have recognised that police use of LFR gives rise to "*significant civil liberties concerns*". That is so in light of both the nature of the technology and uses to which it may be put by the police. It is critical to understand the basis of those concerns in order to determine what constraints are required to meet them.

28. LFR involves processing of individuals' image and extraction of their facial biometric data, which concerns one of the "*chief attributes*" of an individual's personality because it "*reveals the person's unique characteristics and distinguishes the person from his or her peers"* (*Glukhin* §66). Police can deploy LFR "*without requiring the co-operation or knowledge of the subject or the use of force, and can be obtained on a mass scale*" (*Bridges CA* §43) in circumstances where the "*overwhelming majority*" of persons whose

biometrics are captured and processed are not suspected of any wrongdoing (*Bridges CA* §36). That can occur on a mass scale. These characteristics of LFR led the UN High Commissioner for Human Rights to warn in 2023 that "*[f]acial recognition systems … can turn into mass surveillance of our public spaces, destroying any concept of privacy*" (Carlo 1, 30) [CB/296]. Further, as illustrated by Mr Thompson's experience when was mis-identified by LFR, false alerts can lead to people being subject to intrusive questioning and being required to prove they *not* the person an LFR system has assessed them to be (Thompson 1, 18-30) [CB/284]. Thus, as the High Commissioner has observed in a report which was cited with approval by the ECtHR in *Glukhin* at §35, "*even low rates of error*" gives rise to "*significant risks for the enjoyment of human rights*".[7]

29. *Bridges* concerned the deployment of LFR more than 7 years ago. Since then, the tempo and scale of police use of LFR have increased exponentially.[8] The suggestion that this is *less* intrusive than SWP's use of that technology was seven years ago is, therefore, unsustainable (cf. DGD/53). The Claimants agree with the EHRC's submission that the extent of the intrusion into privacy rights will need to be (re)assessed with reference to the way that LFR is being used by the MPS (EHRC/7, 9, 16-24).

30. As set out above, the CA in *Bridges* considered that it was not sufficient, for the purpose of ensuring the interference occasioned by the use of LFR IAWL, that: (a) LFR could only be used where strictly necessary for law enforcement purposes; (b) that there were legal requirements that its use was proportionate, and (c) that it was subject to a process of authorisation as well as other constraints. The CA determined that there needed to be additional and specific constraints on the exercise of discretion as regards the who and where requirements. This begs a key question: why must the police's discretion be constrained in relation to the who and where questions? Why is it not sufficient

[7] UN High Commissioner for Human Rights, *"Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests",* A/HRC/44/24 (24 June 2020) §31. [SB/304]

[8] That is so in respect to: (a) the number of deployments (the SWP used LFR on 50 occasions in the period considered in *Bridges*, the MPS has used LFR nearly 300 times since this claim was issued); (b) the number of people's faces who are scanned during each deployment (almost 40,000 in some single deployments in 2025, SWP estimated that it may have scanned, at most, up to 21,500 faces on a single day); and (c) watchlist sizes (up from a maximum of 800 in *Bridges* to nearly 17,000 in the context of the Defendant's use of LFR), which as the EHRC explains means that facial biometrics are being processed on a vastly greater scale.

that the police are required to act proportionately? What are the civil liberties concerns those additional requirements are meant to meet? That is important. If we can identify the concerns that underpin the "*where*" and "*who*" requirements we can determine whether the constraints applicable to them in MPS' Policy are sufficient to meet them.

31. The reason for the "*who*" requirement is clear. It serves to protect against people being selected for a watchlist for reasons that are arbitrary, discriminatory or without sufficient basis. As to the "*where*" requirement, the concern is not with the individuals on the watchlist but the thousands of innocent people who will have their biometric data taken while going about lawful quotidian activities. The concerns are twofold:

    31.1. **First**, as with the "*who*" requirement, constraining officers' discretion as to "*where*" LFR can be used inhibits officers from selecting locations to deploy LFR for reasons that are arbitrary, discriminatory, or have an insufficient basis. That is a safeguard against individual officers selecting areas arbitrarily or improperly targeting areas where people of certain races or religions disproportionately live or consistently targeting deprived communities in London.

    31.2. **Second**, if there are insufficient constraints on "*where*" the police can use LFR, such that any transport hub, high street or other public location can be targeted, it will be impossible for people to travel across London without their biometric data being taken and processed. Any public place risks becoming one in which people's identities are liable to be checked to see if they are of interest to the police. That would be to fundamentally transform public spaces and people's relationship with the police, and that appears to be the concern which animated the CA in *Bridges*. The CA was concerned about officers selecting deployment locations on the basis of their being places with large footfall, referring to SWP's "*intention during each deployment to allow [the system] to enrol and process as many individuals as possible*" (*Bridges CA* §16). The Court observed that SWP had deployed LFR "*in all event types ranging from high volume music and sporting events to indoor arenas*" which it held "*underlines the concern that we have in this context*" (*Bridges CA* §130). It was to avoid this kind of unconstrained use of LFR, and targeting of public places simply because people congregate there, that the Court of Appeal

held there likely needed to be a connection between the "*where*" and "*who*" questions for LFR to be lawfully deployed.

32. The Defendant does not seek to explain the "where" requirement or identify the concerns it is designed to meet. Instead, he seeks to downplay the significance of police use of LFR:

32.1. The Defendant submits that LFR has a "*negligible*" impact on privacy rights, relying on a finding of the Court of Appeal on whether interferences with Mr Bridges' rights at two individual LFR deployments were disproportionate (DGD/51). That finding concerned the impact of the use of LFR against just *one* individual on *two* occasions and it was made for the purpose of determining proportionality of the interferences with his individual rights. The concern the IAWL requirement seeks to meet in this context is quite different. For the purpose of the IAWL requirement it is critical if there is mass use of LFR to repeatedly process the biometric data of millions of people with the capacity to transform public spaces. As explained above, when considering what is required in terms of constraints and safeguards to ensure a measure is IAWL, the Court must consider, among other things, the number of people a measure affects, and not a single individual's rights.

32.2. The Defendant states that members of the public are "*typically*" or "*generally at liberty to avoid the relevant LFR area*" (DGD/52(i)). Many people, however, will have little choice but to pass through particular spaces when engaging in day-to-day activities. As Ms Carlo explains in her evidence, it is commonly not realistic for people to avoid areas in which LFR is deployed (Carlo 5/5-7) [CB/314]. Even it is possible for an individual to avoid a location where LFR is being deployed prior to being scanned, there is nothing in the Policy which prevents officers from using the fact that someone has tried to avoid the zone to which LFR is being used as a basis for subjecting them to questioning or stopping them (Carlo 5/16) [CB/316].

32.3. The Defendant suggests that as individuals' "*familiarity*" with LFR increases, LFR can properly be considered less rights intrusive (DGD/54(iv)). It cannot be right as a matter of principle that the more frequently or widely a state subjects its population to biometric

surveillance which interferes with their rights that the surveillance becomes *less* intrusive or should be subject to *less* stringent safeguards.

H. THE CLAIMANTS' SUBMISSIONS ON THE GROUNDS

H1. GROUND 1: BREACH OF ECHR ARTICLE 8

First issue: what is the correct approach to the applicable legal principles?

33. There is a dispute of law between the parties as to the correct approach to the IAWL requirement. The Claimants' case is that a key aspect of the IAWL requirement is that discretionary powers must be *sufficiently* constrained such as not to confer an "*excessively broad"* discretion on decision-makers (see above, para 20). Applying this approach, the key issue in this case is whether the constraints on officers' discretion on where to deploy LFR are *sufficient* to ensure LFR is IAWL or whether officers have too broad a discretion.

34. The Defendant, by contrast, maintains that the *sufficiency* of the constraints on the exercise of officers' discretion is not an IAWL issue at all. He argues that provided officers' discretion is not unconstrained, the *extent* of the discretion is relevant only to proportionality. On this analysis, however broad a discretion is conferred on officers, it cannot prevent a power being IAWL provided the only that discretion is not entirely unfettered. That approach to the IAWL test runs through the Defendant's response to this claim. The Defendant asserts, repeatedly, that the issue for the Court in any case where a measure is impugned on the basis it is not IAWL is not the *extent* of the discretion afforded to the decision-maker (DGD/49, 56, 61, 64(iii), 68, 75). Rather, the Court only needs to be satisfied there is *a* constraint on the exercise of the decision-makers discretion, without having regard to the adequacy or extent of that constraint. Thus, the Defendant asserts that "*so long as the Court is satisfied there is not unfettered discretion on the constable deciding where to locate LFR, [there] is not a maintainable legality challenge*" (DGD/75). He asserts that provided "*there are no parts of the Policy that allow unfettered discretion for an officer to add whomever he or she wants to a watchlist or place the LFR camera wherever he or she wishes … there is no maintainable attack on the Policy as lacking the quality of law*" (DGD/68). He asserts, that the "*breadth"* of the discretion conferred on an officer to choose where to locate LFR does not go to the legality of its use and is only relevant to proportionality (DGD/68).

35. The Defendant's case on this point of principle is based on a misreading of the authorities on the application of the IAWL test to discretionary powers. It is wrong for the following reasons:

36. **First**, it is clear from the domestic and Strasbourg authorities that the breadth or degree of discretion afforded to the decision maker – in other words, its *extent* – is central to the assessment of whether the IAWL requirements are met. That is why, for example, challenges such as *Gillan* and *AR* succeeded:

36.1. In *Gillan*, the ECtHR was concerned by the "*breadth of the discretion*" conferred on officers to conduct stops and carry out searches under s 44 of the Terrorism Act 2000 (§83). The Court concluded the measure failed to comply with the IAWL requirement, even though a search could only be carried out for the purpose of looking for articles which could be used in connection with terrorism, because this was a "*very wide category which could cover many articles commonly carried by people in the streets"* (*ibid*). Thus, while officers' discretion to conduct stops and searches under s 44 of the Terrorism Act 2000 was not unfettered, its breadth gave rise to a *"clear risk of arbitrariness*" which meant there was a breach of Article 8 (§85).

36.2. Similarly, in *AR,* the Government argued that the scheme relating to the disclosure of information (on Enhanced Criminal Records Certificates) that an individual had been charged and acquitted of a serious sexual offence had a number of "*built-in safeguards including that information would only be disclosed where the police reasonably believed that it was relevant to the certificate and ought to be included following consideration of each particular piece of information*" (§59). The ECtHR concluded that despite those constraints, again, the applicable law and guidance still left an "*excessively broad discretion*" to the decision-maker and was attended by "*insufficient safeguards*" (§68). It therefore fell-foul of the IAWL test.

37. The distinction the Defendant seeks to draw between cases in which there are, on the one hand, *no* constraints on the exercise of a discretionary power (which he appears to accept would give rise to an IAWL problem) and, on the other, those where there are *some* constraints but an individual alleges these are insufficient (which, he says, cannot be challenged on IAWL grounds) cannot,

therefore, be reconciled with the established principles which have developed in the case law. It is clear from the authorities that the task for the Court in considering whether a discretion afforded to officers is *sufficiently* circumscribed is squarely a legality issue and that is why the courts repeatedly stress that the question is whether there is "*too much latitude*" (*Domenichini* §32) or "*too much discretion left to individual police officers" (Bridges CA* §91), and not whether a discretion is unfettered.

38. **Second**, the Defendant's position is wrong in principle. Suppose an LFR policy allowed anyone to be added to a watchlist who satisfied certain criteria and, on analysis, the criteria covered 90 or 95% of the population. The discretion conferred on individual officers to choose who they wished would be extremely broad albeit not unfettered. That would clearly be relevant to whether police had "*too much discretion"* or "*too much latitude"* and whether there were sufficient constraints to prevent individuals being arbitrarily or improperly targeted.

39. **Third**, the Defendant's analysis is based on a misreading of *In re Gallagher* [2020] AC 185. He relies on a handful of sentences in Lord Sumption's decision, shorn of their relevant context, to assert that insofar as a decision-maker's discretion is confined by some rules and by reference to particular principles, the extent of a public authorities' discretion does not give rise to a legality issue (DGD/48-49).

40. The context of *Gallagher* is important. It involved challenges to legislation which compelled the disclosure of information relating to spent convictions and cautions in certain situations (for example where a person had two or more convictions/cautions of any kind or a conviction for any violent offence). The challenge was to bright-line rules, which applied automatically, and not to the exercise of any discretionary power. In advancing that argument, the Defendant misreads Lord Sumption's observations in *Gallagher*:

    40.1. The Defendant relies on comments made by Lord Sumption in respect of *compulsory* rules and misapplies them to an analysis of *discretionary* powers. When Lord Sumption noted, in respect of the legislative scheme governing the disclosure of conviction information, that there may be arguments for fewer, wider, or narrower categories of conviction information but the legality test is a "*fundamentally unsuitable instrument*

for assessing differences of degree" (*Gallagher* §44), cited at (DGD/48)), he was referring to legality challenges to *compulsory* rules. That is clear when the comments are read in the context of Lord Sumption's wider discussion of the IAWL test and bright-line rules. Lord Sumption's comments did not concern discretionary powers, where, as summarised above at §19-21 above, questions of the degree of discretion afforded to decision-makers are critical. Nowhere in *Gallagher* does Lord Sumption suggest that a *discretionary* measure cannot be a challenged on the basis that it fails to meet the IAWL test because the degree of discretion afforded to a public authority is too broad.

40.2. Lord Sumption's analysis refers to, and relies upon, the various authorities in which discretionary powers were held not to comply with the IAWL test on the basis that discretion conferred on public authorities was not sufficiently constrained. That includes *Gillan* and *MM v United Kingdom*, App No 24029/07, 29 April 2013, cited by Lord Sumption in *Gallagher* at §24-29. Thus, *Gallagher* cannot be read to mean that powers can no longer be impugned as not being IAWL on the basis that the extent of the discretion they confer on decision-makers is too broad.

40.3. The Defendant notes that Lord Sumption referred to the condition of legality as being "*binary*" (*Gallagher* §, cited at (DGD/48)). That is, of course, correct. A measure either has the quality of law or it does not. That is consistent with the Court's task of assessing whether constraints on a discretionary power are sufficient for the purpose of the IAWL requirement. Where a discretionary measure is challenged as not being IAWL, a Court must evaluate, among other things, whether the IAWL requirements set out above at §19-20 are satisfied. Having undertaken that evaluative exercise, a Court will reach the conclusion that the measure either complies with the IAWL requirement, or it does not. If a measure is not IAWL because, for example, a public authority is left with too much discretion or latitude, it follows that until relevant defects are remedied its application would breach the ECHR rights of those affected. That is a binary judgment but based on the Court's evaluation of the *extent* of the discretion conferred and whether it is too broad given the nature of the power, the numbers affected etc.

Second issue: Are there sufficient constraints on the MPS' discretion to use LFR?

41. If the Claimants are correct on the law, the question is whether the legal framework governing the MPS' use of LFR sufficiently constrains police officers' discretion as to where LFR can be located. Or are officers left with too much discretion? The Claimants make four points in that regard, which are developed below:

    41.1. The Defendant relies on aspects of the Policy in respect of the purposes for which LFR can be deployed and requirements to consider the proportionality of deployments to argue that the "where" requirement is satisfied. They do not meaningfully constrain the discretion as to where LFR can be located, and substantially the same provisions were considered to be insufficient in *Bridges*.

    41.2. The MPS' "*use cases*" are intended to circumscribe where LFR can be located. On proper analysis, however, they confer far too broad a discretion on individual officers, and permit them to deploy LFR anywhere they choose in the significant majority, if not the vast majority, of public spaces in the Metropolitan Police District ("**MPD**") at any time. That is little different to the position to the position in *Bridges* and is too broad a discretion to ensure use of LFR is IAWL.

    41.3. The Policy permits officers to designate an area as a "*hotspot*" based on "*operational experience as to future criminality*". That is opaque and entirely subjective. It does not provide a meaningful constraint on officers' discretion to use LFR and renders its use unforeseeable to those whose rights may affected.

    41.4. Contrary to *Bridges CA*, there is no requirement for there be any connection between where officers choose to locate LFR and the persons sought (i.e. those on watchlist) through a deployment of LFR.

The Defendant's reliance on "why" and "whether" constraints

42. Before turning to the submissions on the "use cases" in the Policy that purport to confine where LFR can be used, it is necessary to deal with the Defendant's assertion that other aspects of the Policy provide significant constraints on his

officers' discretion as to where LFR can be located. He relies on what he calls the "why" and the "whether" of LFR deployments.

43. Dealing with the '**why**' first, the primary policing objective which runs through the use cases is "*locating sought persons*," with an additional permitted objective in PSO / event use cases of deterring or disrupting the attendance of those who pose a threat (DGD/37(i), 38(i), 39(i); Policy §2.5, 2.8, 2.10) [CB/186-187]. The Defendant refers to this as the 'why' of LFR deployment and he avers that *"[i]t is the why that determines the location…"* (DGD/37(i), 82). The Defendant suggests that this "contrasts" with the position in *Bridges* because it "*confines [LFR deployments] to particular policing objectives are advanced*" (DGD/35, 81).

44. There are two problems with this submission.

    44.1. First, the Defendant's attempt to draw a distinction with *Bridges* is misconceived. SWP was required to deploy LFR for policing purposes. Apart from anything else, that was required by data protection legislation (see *Bridges DC* §85-87, 128). It is apparent from the DC's judgment that SWP used LFR to locate wanted persons and to deter disorder (*Bridges DC* §11, 13), these are objectives that are akin to the MPS' Use Case A and the events PSO under Use Case B. The CA did not accept that restrictions on the use of LFR for policing purposes was a sufficient constraint on the discretion as to where LFR could be located.

    44.2. Second, the essence of the Defendant's 'why' is to locate persons on watchlists. With the exception of the requirement that there must be intelligence indicating that one person eligible for inclusion on a watchlist will present during a Use Case C deployment, there is no requirement for any connection between watch-listed persons and the deployment location. The Defendant is therefore incorrect in suggesting that a requirement that LFR be deployed for locating sought persons (which is all that is required under Use Case A) determines the location and is a meaningful constraint on where LFR can be located.

45. Turning to the '**whether**' question, it concerns a requirement for "*decision-makers to assess proportionality in Section 6 of the policy, which includes consideration of engaged Convention rights … and a staged process to*

determine the extent to which the deployment will advance policing objectives, the availability of both LFR and non-LFR alternatives, and whether the proposed Deployment strikes a fair balance" (DGD/37(iv), 38(iv), 39(iv)). Section 6 of the Policy requires authorising officers to "*consider whether ether proposed deployment would be a proportionate means of achieving the MPS' policing objectives in light of the impact of deployment on the rights and freedoms of members of public*"[9] (§6.1). The Policy directs officers to undertake a proportionality analysis (§6.7-6.10).

46. This amounts to a policy direction to comply with the MPS' statutory obligations under s 6 of the HRA 1998 and data protection law. That cannot suffice. The same legal requirements on proportionality applied to SWP's use of the LFR in *Bridges.* While they were not contained in SWP's standard operating procedures (save in relation to watchlists), they were still part of the legal framework governing LFR. Furthermore, the Surveillance Camera Code (on which SWP relied) contains requirements around the use of LFR being proportionate to the purposes pursued, and data protection legislation placed a duty on SWP to process biometric personal data only where that necessary (and thus proportionate) for law enforcement purposes (see *Bridges DC* §33, 41, 87 Annex A). The Court did not consider this a sufficient constraint on officer discretion as to where LFR could be deployed.

The extent of the MPD in which the Policy permits LFR to be deployed

47. The relevant constraints on 'where' officers can exercise their discretion to locate LFR are in his three "use cases". These purport to circumscribe where in the MPD LFR can be deployed. The Defendant has not calculated the extent to which the use cases actually restrict officers' choice of where to locate LFR. As set out below, however, the evidence suggests that under the Policy's use cases, officers can deploy LFR anywhere they choose in the significant majority, if not the vast majority, of the public spaces in the MPD at any time. While the Policy contains detailed provisions on where LFR can be located, they, in fact, provide little if any constraint on officers' discretion. That is because it appears most of the city is covered by one or other of the Defendant's use cases. That is little different to *Bridges* and is too broad a discretion to satisfy the IAWL requirement.

[9] The Policy makes it clear that the rights in question are Convention rights (¶6.4).

The Defendant's criticisms of the Claimants' reliance on 'quantitative' considerations

48. Before explaining why that is so, it is necessary to address the Defendant's assertion that the "*proportion of London … covered*" by the Policy's Use cases is not "*relevant*" and is an "*arid*" discussion (DGD/7(ii)(d)). That, says the Defendant, is because "*the question whether the Policy has the quality of law is necessarily qualitative not quantitative*" (DGD/7(ii)(d)); reference to "*quantitative*" considerations "*confuses legality [i.e. the IAWL requirement] with proportionality*"; and "*breadth*" of a discretionary power cannot be impugned on IAWL grounds (DGD/59-60, 68). The Defendant says, therefore, that evidence as to the proportion of the MPD in which LFR can be located is "*unnecessary and unhelpful*" (DGD/66) and the "*vast majority"* of the expert evidence of Prof Utley is "*irrelevant"* (DGD/9(i)).

49. This argument is misconceived. It is premised on the Defendant's interpretation of *Gallagher* and the IAWL case law on discretionary measures is wrong. Since the key issue is whether or not an officer's discretion as to where to locate LFR is *sufficiently* constrained, it is necessary to understand how/to what extent the Policy actually imposes constraint. If, on analysis, an LFR policy, allows officers to deploy LFR anywhere they choose within 95% of the public spaces in the MPD at any time, that is plainly relevant to whether "*too much discretion"* has been conferred in relation to the "where" question. On the Defendant's analysis, provided a policy is "*detailed and prescriptive"* (DGD/20), the fact that it operated so that LFR could, in fact, be deployed anywhere in 99% of the public places in the MPD could not prevent it being IAWL. That cannot be correct. As to the need for expert evidence, given that the Policy purports to impose constraints with reference to spatial and data-based concepts, it is not possible from simply reading the policy to determine how far it actually constrains officers' ability to choose where to locate LFR. The extent of that discretion can only properly be understood with the assistance of expert analysis.[10].

The extent of the discretion to use LFR at "crime hotspots"

50. How far, then, does the Policy constrain where LFR can be located? In his second report Prof Utley examined what proportion of the MPD and the Central North

[10] That evidence is contained in the second and third reports of Prof Utley, as well as evidence of the MPS' statisticians which Ms Chiswick summarises in her own statement (Chiswick 2/107-108) [CB/347].

BCU (as an example) would be covered the "crime hotspots" part of Use Case A, assessed on the basis of crime data and crime rising metrics or contain access routes to those hotspots (Utley 2/3.1, 4.1-4.7 and Appendix A) [CB/371]. Prof Utley estimated that 47% of the MPD could be labelled as a "*crime hotspot*" (meaning LFR could be located there) and LFR could be deployed on access routes to these hotspots lying within a further 38% of the MPD; that gave a total figure of 85% of the MPD that was either a crime hotspot or contained access routes to crime hotspots (Utley 2/4.5, A.6) CB/373, 387]. The same estimate for the Central North BCU was 89%, 51% falling within crime hotspots and 38% falling within the 300m radius of crime hotspots (Utley 2/4.5, A.4-5) [CB/373, 383-385]. Prof Utley was not in a position to estimate in what *additional* proportion of the MPD in which the MPS could locate LFR based on the OCU crime hotspots, crime hotspots selected on the basis of intelligence or operational experience, or missing persons hotspots of Use Case A, or any part of Use Cases B and C.

51. In his DGD and evidence, the Defendant took issue with Prof Utley's analysis, including in respect of "*assumptions made about how the Defendant operationalises the policy*" (DGD/67). This was on the basis that, in summary: (i) the MPS calculates crime rates according to three indicators which means that there are no "ties" between areas within a BCU; (ii) the MPS uses a different "*more sophisticated*" approach to assessing rates of rising crime (Prof Utley used the MPS' crime data with reference to month-to-month increases, whereas Ms Chiswick says "crime rising" is calculated by comparing the most recent year of crime data with the previous two years); (iii) the placement of grid for hotspots has been fixed since September 2024 and is not altered by officers; (iv) with reference to access routes, Prof Utley was alleged (wrongly, see below) to have assumed that LFR could be deployed at every point within the 300m radius around hotspots; and (v) his analysis was undertaken with reference to whole of the MPD rather than areas in which LFR is "*practically deployable, having regard to physical constraints and the need for publicly accessing space*" (DGD/67; Chiswick 2/91-114) [CB/343-350].

52. There are four features of this response.

    52.1. First, none of these purported additional constraints (points (i)-(iii) and (v)) is set out in the Policy or any other document governing, and thus

constraining, officers' exercise of the discretion to use LFR. They are therefore not relevant to the IAWL requirement.

52.2. Second, these points make little difference to the assessment of the percentage of the MPD in which officers can exercise their discretion to locate LFR at crime hotspots. Ms Chiswick accepts that on the MPS' own analysis LFR can be located in around 40% of the MPD (compared to Prof Utley's estimate of 47%) on this basis (Chiswick 2/102) [CB/346].

52.3. Third, the suggestion that Prof Utley asserted that every point within a 300m radius of a hotspot was an "access route" is wrong. It misreads his report (Utley 3/4.1-4.7) [CB/410-412].

52.4. Fourth, as to an analysis of the parts of the MPD at which LFR is "*practically deployable*", that, in fact, yields relatively similar results to Prof Utley's analysis relating to the whole of the MPD. In any event, as set out below, given the additional information the Defendant has now provided, Prof Utley has undertaken further calculations by reference to practically deployable areas.

53. Upon receiving Ms Chiswick's statement and further statistical information in a letter (dated 5 November 2025 [CB/424] and [CB/433]), the Claimants instructed Prof Utley to undertake further analysis. Recognising that it may be more meaningful to consider the proportion of the potentially deployable areas of the MPD (i.e. roads, paths, tracks or roadside *and* not areas where LFR cannot be physically deployed, such as rivers, private buildings and other places without public access: "**deployable parts**"),[11] Prof Utley was asked examined the proportion of deployable parts of the MPD in which the Defendant's officers could deploy LFR on the crime hotspots basis. This evidence shows that under the crime hotspot use case alone, "*of the total area in which LFR is physically potentially deployable* [i.e the deployable parts] *within the MPS District … approximately 52% lies within 'crime hotspot' where LFR can be used"* – the same figure for the Central North BCU was 47% (Utley 3/3.6-3.7) [CB/409-410]. Those figures are not understood to be disputed and are, in fact, higher than the figures obtained by examining the entire area covered by hotspots.

The discretion to use LFR on access routes to crime hotspots

[11] See Chiswick 2/107 and Utley 3/3.2-3.4 and the Defendant's letter of 5 November 2025.

54. In addition to locating LFR at crime hotspots, officers can locate LFR at any "*access route within an approximately 300m radius of a hotspot location*" (Policy §5.2) [CB/191] That term is not defined in the Policy. Ms Chiswick's evidence is that the MPS interprets an access route as one "*which members of the public are in practice likely to use to access the hotspot: for instance, the main road to a hotspot from a nearby station*," and not "*points or roads which a member of the public could, by some circuitous or unlikely route, access the hotspot*" (Chiswick 2/105; DGD/67(iv) [CB/347]. As the Claimants understand it, this means officers exercise an evaluative judgement as to whether a route satisfies the criterion, and, in particular, whether it is something akin to a *"main road to a hotspot from a nearby station"*. That, however, appears nowhere in the Policy and is not, as a matter of ordinary language, what "*access route*" means. An "*access route*" is a "*route"* by which someone can "*access*" a place and is clearly not limited, on an ordinary understanding, to things like main roads or routes from public transport hubs. That means that a significant number of roads in the 300m around a 300-500m wide "*crime hotspot*" will be "*access routes"* to the hotspot.

55. Even on the Defendant's own, restrictive interpretation of an access route (Chiswick 2/107) [CB/347], LFR can be located in an estimated additional 10% of the deployable parts of the MPD (and 9% of the Central North BCU) on the basis that it is an access route to a crime hotspot (Utley 3/3.6-3.7) [CB/409].[12] That means officers can deploy LFR anywhere within 62%, i.e. nearly 2/3, of the publicly accessible parts of the MPD at any time. As set out above, it is apparent, however, that the ordinary meaning of "*access routes*" is broader than Ms Chiswick suggests MPS is currently applying. It could cover far more than an additional 10% of the deployable parts of the MPD. Taking a conservative estimate, it could add another 15-20% to the area in which LFR can be deployed.

Other locations where LFR can be deployed

56. The previous subsection considered only deployment by reference to "crime hotspots" in BCUs calculated by reference to "crime data". There are, however, numerous other bases on which LFR can be deployed which significantly further expands officers' discretion as to where to locate LFR (see Policy §2.3-2/9;

[12] The MPS officers applied "*using their operational judgement and knowledge to identify any access routes to a hex*" to determine access routes in the Central North BCU (letter of 5 November 2025 §18) [CB/424].

SFG/131-136) [CB/186]. The additional use cases are: (a) crime hotspots which are selected on the basis that (i) "*intelligence reporting*" and/or (ii) "*operational experience as to future criminality*" indicates an area is in the upper quartile for crime rate or rising crime (under Use Case A); (b) crime hotspots in OCUs (Chiswick 2/51) (under Use Case A); (c) missing persons hotspots (under Use Case A); (d) the use of LFR in support of "*protective security operations*" (i) within 300m of critical national infrastructure, and (ii) at events (under Use Case B); and (c) where there is specific intelligence that one or more people on a watchlist is likely to be at the deployment location (Use Case C).

Conclusion on extent of the MPD in which the Policy permits LFR to be deployed

57. As set out above, 52% of the "deployable part" of the MPD is a "crime hotspot" in which LFR can be deployed, increasing to 60% or 70% once access routes are added. The Defendant has not disclosed (if, indeed, his officers have ever assessed) what additional proportion of the MPD officers have a discretion to use LFR in pursuant to use cases beyond crime hotspots, and that cannot be calculated by any publicly available documents. If, however, those Use Cases increase the locations where LFR can be deployed by 10 or 20%, that would mean officers are able to select anywhere within over 70%, 80% or 90% of the public spaces in the MPD to deploy LFR. That may be marginally different to *Bridges* where there was no express constraint in SWP's policies on where LFR could be located, but in practice it is little different. In both cases "*too much discretion [is] left to individual police officers" (Bridges CA* §91). Given the civil liberties concerns that the "*where"* requirement is intended to meet (see §31) allowing the police to select anywhere they wish within a significant majority of the MPD at any time to deploy LFR means its use is insufficiently constrained to be IAWL.

Discretion to locate LFR on the basis of intelligence reporting and operational experience

58. The Policy permits officers to designate a 300-500m area as a crime hotspot on the basis that "*operational experience as to future criminality indicates that that it is an area where the crime rate and/or the rate at which crime is rising is assessed to be in the upper quartile for that BCU/OCU"* (§2.3) [CB/186]. That is opaque and subjective and provides far too broad a discretion to officers to

select an area for LFR deployment and it is not possible to meaningfully foresee its exercise.

The lack of a connection between the 'who' and the 'where' questions

59. As explained above, in *Bridges* the Court was concerned about the lack of a connection between the location of LFR and persons included on a watchlist. With one exception, there is no requirement under the Policy for any connection between watchlisted persons and deployment location. [13] Officers need not have any reason to think that any of the "sought persons" on a watchlist for a given deployment will be present in that place during a deployment. That is not consistent with *Bridges.*

60. The Defendant argues that the CA was simply "*speculating as to one possible example of how a hypothetical policy might satisfy the legality requirement*", and were not seeking to "*dictate*" the contents of an LFR policy (DGD/79(i)]. That misses the point. There are two ways LFR can be deployed. It can be used in a targeted way. For example, if the police have reasonable grounds to suspect that particular individuals were going to engage in violence at a football game, they could be placed on a watchlist and LFR used to detect their presence in the vicinity. Or LFR can be deployed in a mass and untargeted way, selecting areas where a very large number of people are likely to pass and using a very large watchlist, in the hope that someone on the list will happen to pass by. The CA may not have sought to "*dictate"* precisely how an LFR policy was formulated but it was clearly concerned about the latter way of using LFR and considered that the IAWL requirement should constrain. Otherwise, its references to the who/where connection make little sense. The Defendant considers that constraining mass and untargeted use of LFR would "*substantially deprive LFR of its utility to the police: the whole point, in most use cases, is to locate people whose location the police do not know*" (DGD/79(iii)), and it is clear that he uses large watchlists (much larger than used by SWP) at crowded locations in the hope of positive matches. He sets out in detail the perceived disadvantages of being prevented from operating LFR in that way (DGD/82-92). But it was precisely such mass and untargeted use that concerned the CA in *Bridges*, which discretion it considered had to be constrained.

[13] That exception is Use Case C but, as set out above, there need only be a connection in respect of one individual and the deployment location.

61. The Defendant also states that the Court was only concerned that at least *someone* on the Watchlist was suspected of being present at the location (DGD/79(iii)), and would have been content with a policy that imposed such a requirement. That is clearly wrong and reflects the vice of the Defendant's previous LFR policy. The previous policy required the police to have "*reasonable grounds*" to suspect that "*one or more persons on the Watchlist*" would be present when LFR is deployed (see SFG/73). As Prof Utley's first report showed, with a large watchlist, of the size the Defendant was using (and even if the police know nothing about where those people are located beyond that they are believed to be in London), if they deploy LFR at any crowded location they will almost always expect to find at least someone they are looking for (SFG/83). As noted above, following the Claimants issuing of proceedings and receipt of Prof Utley's report the Defendant substantially changed its LFR policy.

H2. GROUND 2: BREACH OF ARTICLES 10 AND 11 ECHR

62. Ms Carlo also challenges the MPS use of LFR on the basis it is not PBL pursuant to Articles 10 and 11 ECHR. The Policy contemplates the use of LFR at protests (Policy/ 6.5(b)(i)) [CB/193]. The MPS has not disclosed whether LFR has already been used at any protests in London, though Ms Chiswick asserts that the decision on whether to deploy LFR at protests "*is always a dynamic one*" taken on the basis of the "*facts specific to that event*" (Chiswick 2/71 [CB/339].

63. The Defendant accepts that his use of LFR is capable of interfering with the Article 10/11 rights of individuals attending protests (DGD/93). In that regard, there is an interference with Articles 10 and 11 rights not only engaged when individuals attend a protest are subject to LFR, but also where the use of LFR is "*capable of having*" a "*chilling effect*" on the exercise of expression and association (*Baczkowski v Poland*, App. No. 1543/06, 3 May 2007 §67; *Various Claimants v NGN* [2019] EWCA Civ 350 §18).[14] In *Glukhin*, the Strasbourg Court specifically acknowledged that the use of "*highly intrusive facial recognition technology to identify and arrest participants in peaceful protest actions could have a chilling effect in relation to the rights to freedom of expression and assembly*" (§88).

[14] Having a chilling effect has been described as having at "*deterrent impact"* on a person exercising their rights (*R (Leigh) v Commissioner of Police of the Metropolis* [2022] 1 WLR 3141 §76).

64. Given the broad discretion accorded to police officers on where to locate LFR, it can be used in circumstances in which it will interfere not only with Article 8 rights but Article 10/11 rights. That further increases the need for sufficient constraints on that discretion. If, for the reasons above, there are insufficient constraints for the purpose of Article 8, the position will be *a fortiori* once the additional impact on Article 10/11 rights is considered.

I. CONCLUSION

65. For the foregoing reasons, the Claimants respectfully invite the Court to grant the application for judicial review and to grant declaratory relief in the terms sought.

DAN SQUIRES KC
AIDAN WILLS
ROSALIND COMYN
Matrix
5 December 2025