Response to the UK Government's Consultation on New legal framework for Law Enforcement Use of Biometrics, Facial Recognition and Similar Technologies

Dr. Asress Gikay
Senior Lecturer in AI, Disruptive Innovation and Law
Brunel University of London
asress.gikay@brunel.ac.uk

January 12, 2026

Executive Summary

- The new legal framework should set out a proportionate, evidence-based, and context-sensitive governance framework for the use of biometric and inferential technologies by law enforcement authorities.
- To ensure agility, a layered approach should be adopted, combining primary legislation that sets out general rules, oversight mechanisms, and key safeguards, with secondary legal instruments that provide detailed rules for specific use cases.
- Four-pronged graduated proportionality assessment rules should be introduced, setting legal thresholds for the use of biometric and inferential technologies, and excluding certain categories of criminal offences from justifying deployment.
- Graduated deployment authorisation rules should be introduced, where the current internal authorisation process for facial recognition technology is supplemented by independent authorisation for specified deployments that require heightened independent scrutiny.
- A risk-based, tiered authorisation model should apply to facial recognition searches of non-law-enforcement databases.
- An independent oversight body should be created that, amongst others, sets and enforces regulatory standards, and a one-stop-shop complaints and redress mechanism for affected persons.

Policy Context and Approach

The Home Office's public consultation (Home Office, 2025) to develop a legal framework for the use of facial recognition technology (FRT) and other biometric technologies for law enforcement is timely. Effective regulation is necessary for improving public safety, protecting people's rights, ensuring transparency and accountability in the use of new technologies by law enforcement authorities, and building public trust.

The call provides an opportunity to the government to consider diverse viewpoints as well as the available evidence and make informed policy choices. Current proposals commonly include blanket prohibition of the use of FRT in public spaces (e.g., Matthew Ryder, 2022) or a moratorium (e.g., Pete Fussey and Daragh Murray, 2025 and Big Brother

Watch, 2020) and the prohibition of predictive policing AI tools (Amnesty International, 2025).

These proposals largely perpetuate a historical pattern where campaign groups and academics oppose security technologies, including CCTV cameras, which are now widely considered indispensable tools for solving crimes (*see* Asress Adimi Gikay, 2025). If adopted, these proposals would have made it impossible for UK law enforcement authorities to gain the valuable experience in safely deploying FRT over the past several years, including arresting over 900 wanted persons in a single year (Metropolitan Police Live Facial Recognition Annual Report, 2025) and conducting two independent equitability audits.

While stripping law enforcement authorities of effective public safety tools, bans and moratoria preclude generating the empirical evidence necessary for designing effective regulation, including safeguards against bias and other relevant risks. The same opponents of surveillance technology are likely to switch gears and advance a new set of equally unrealistic proposals that, through unjustifiable red tape, excessive restrictions and unworkable standards, would render facial recognition and other biometric technologies ineffective.

Regulation should be grounded in context-sensitive, real-world evidence, not in academic theories untested in operational environments or one-sided narratives promoted by self-interested groups.

Informed by extensive research, my recommendations are guided by five principles that indicate the effectiveness of the proposed legal framework:

1. Measured/proportionate— The new legal framework should be based on weighing of the risks including risks to human rights and benefits of various policing AI technologies to adopt proportionate regulation that balances competing societal interests.
2. Evidence-based—The new legal framework should be grounded in demonstrable evidence of technical performance, effectiveness and risk profile.
3. Agile— The new legal framework should effectively respond to changing technological and operational developments as well as emerging evidence of risks, to the extent possible, without the need for further statutory intervention.
4. Transparency and public trust— The new legal framework should promote transparency around the use of policing AI technologies to build and sustain public trust.
5. Accountability and redress — The new legal framework should ensure appropriate oversight, accountability, and meaningful mechanisms for redress to individuals for harms from the use of the relevant technologies.

Based on the above principles, the submission sets out workable solutions that can be realistically implemented.

1. To what extent do you agree or disagree that a new legal framework should apply to all use of 'biometric technologies' by law enforcement organisations?

1.1. The new law should apply to FRT and other biometric technologies, provided that each in-scope technology is appropriately regulated, proportionately with its benefits, and risk profile.

1.2. Some biometric technologies used by law enforcement authorities have already demonstrated clear benefits. For example, Live facial recognition (LFR) and retrospective facial recognition (RFR) have proven to be effective in apprehending people suspected of committing crimes, wanted by courts with outstanding arrest warrants or with bail conditions (Metropolitan Police Live Facial Recognition Annual Report, 2025).

1.3. Other technologies may have potential benefits but are not yet tested or proven to be effective. Movement recognition systems could be used in specific contexts, for example in relation to suicide prevention in controlled environments but they are only at an experimental stage (e.g., TFL Trials of Smart Station Willesden Green Station, 2023).

1.4. Due to being at early stage or inherent challenges of the tasks to be performed, certain biometric technologies face serious technical limitations. Emotion recognition systems are a clear example.

1.5. Studies demonstrate that emotion recognition systems struggle to account for cultural differences and the subjectivity as well as context-dependency of facial expressions, voice tones, and other cues to be able to correlate them to a specific meaning such as deception(Lena Podoletz, 2023). By their very nature, they aim to infer people's internal feelings (including mental state) which is difficult to achieve. Due to lack of scientifically reliable methods to validate them, their accuracy and reliability in law enforcement settings are highly questionable.

1.6. At the same time, emotion recognition is among the most intrusive biometric tools, as it purports to assess deeply personal states, invading people's private spaces. Using such technologies in supporting law enforcement requires adherence to strict standards and a high threshold for assessing necessity and proportionality.

1.7. Despite their risks, emotion recognition systems are not categorically banned elsewhere. For instance, in the EU, they are prohibited for use at workplace and education institutions except when used for medical or safety reasons (EU AI Act, Article 5(1)(f)). They are classified as high-risk AI systems in other cases including in law enforcement (EU AI Act, Annex III(1)(c)). This experience suggests that regulation should take a measured approach and enable the responsible development and use of various law enforcement technologies.

1.8. Other tools that have been tried include AI tools that predict where a crime might occur (geographic prediction) or who might commit a crime or be a potential victim of a crime (individual predictive tools), based on profiling— generally called predictive systems. If trained on manipulated, distorted or historically biased data, these tools are susceptible to perpetuate biased policing practices (Rashida Richardson and others, 2019).

1.9. However, when developed and deployed responsibly following strict safeguards, they can offer valuable support to law enforcement in deploying resources effectively and safeguarding public safety.

1.10. Although predictive AI systems may not qualify as biometric technologies in all cases, as they can also rely on non-biometric data such as information regarding the flow of crowds, major events, and other non-personal data (geographic prediction), the new law should still apply to them as well as other biometric technologies used in law enforcement.

1.11. A narrow scope would risk creating gaps as law enforcement technologies evolve, potentially leaving new or evolved systems without a clear legal basis. A broader scope would ensure legal certainty, accountability, and public trust, while also future-proofing the regulatory framework against technological advancements.

1.12. Nevertheless, it is crucial to recognise that different technology use cases present different levels of risk and therefore cannot all be regulated in the same way. It would be neither realistic nor desirable to prescribe detailed rules for every specific use case in primary legislation. Instead, the new legal framework should establish general principles, clear oversight mechanisms, and robust safeguards applicable across all in-scope technologies.

1.13. Detailed and context-specific rules should then be developed through secondary legal instruments, including regulations, codes of practice and local policies.

1.14. This layered regulatory approach ensures agility and aligns with the case law of the European Court of Human Rights (ECtHR), which recognises that the requirement of legality (in assessing lawful interference with human rights, including privacy) may be satisfied by a combination of primary legislation and secondary laws, including codes of practice and administrative rules. These legal instruments must however be accessible, foreseeable, and legally enforceable, and meet the requisite "quality of the law" requirement(Asress Adimi Gikay, 2023a). This principle embraced by most ECtHR decisions is explicitly recognised by UK Supreme Court in Catt(Lord Sumption) (R. (Catt) v Association of Chief Police Officers of England, Wales and Northern Ireland [2015] UKSC 9, [2015] A.C. 1065, at [11]). The ECtHR has not subsequently questioned this principle upon appeal (see Catt v United Kingdom (2019) 68 EHRR 7).

2. Do you think a new legal framework should apply to 'inferential' technology i.e. technology that analyses the body and its movements to infer information about the person, such as their emotions or actions?

2.1. The new legal framework should apply to technologies that make inferences about a person's emotion and actions.

2.2. To ensure legal certainty, avoid future regulatory gaps, and allow law enforcement authorities to deploy new tools where they are proven effective, the new legal framework should also cover inferential tools. For example, it would be beneficial to use a suicide-prevention tool that alerts authorities based on movement patterns in controlled environments such as prisons. Such deployments require legal basis and oversight mechanism.

2.3. Currently, technology providers are developing real-time movement, gesture and behaviour recognition technologies to tackle shoplifting as an alternative to LFR (e.g. Veesion, 2025). Due to its ability to automatically pixelate personal identifying features such as faces, the tool is considered less privacy-intrusive, its focus being on gesture and movement patterns to detect suspicious activities and behaviours. However, whilst such technologies have not yet been tested in law enforcement, the absence of an established legal framework governing their lawful use would make even pilot deployments challenging.

2.4. The proposed approach to extending the law beyond FRT is also consistent with developments in the European Union (EU). Under the EU AI Act, certain inferential and behavioural AI systems used in law enforcement, including AI systems to assess the risk of individuals becoming victims of crime(individual predictive AI), AI systems used to assess the risk of offending or re-offending, other than solely through profiling or personality-based inference are considered as high-risk and are subject to strict regulatory standards for development and deployment(EU AI Act, Annex III(6)).

2.5. Interestingly, geographic crime prediction tools are neither prohibited, nor high risk under the EU AI Act, unless they involve indirect behavioural profiling of individuals. This is despite studies showing that, if trained on data reflecting biased historical policing practice, the system could replicate the same pattern by discriminatorily predicting minoritised neighbourhoods as crime hotspots. It also possible to use objective factors in predicting crime hotspots, but this means that such tools should be subjected to appropriate regulation. The new law should lay the foundation for contextual regulation of these technologies.

2.6. It is worth noting that UK police have trialled predictive AI tools examined by Amnesty International in its report Automated Racism (Amnesty International, 2025). However, the report contains notable methodological weaknesses, including reliance on interviews with an unrepresentative demographic group with a strong predisposition against law enforcement, which undermines the reliability of its conclusions.

2.7. The new law should also cover emotion recognition systems and create relevant standards for their use (see *paras* 1.6 & 1.7).

2.8. Bringing inferential tools within the scope of the new law helps ensure that the legal framework remains fit for purpose as technologies evolve, reduces the risk that emerging tools fall outside regulation, and enables the responsible use of innovative tools in law enforcement.

3. Do you think a new legal framework should apply to technology that can identify a person's clothing or personal belongings, or things that they use (e.g. a vehicle)?

3.1. The new legal framework should apply to technologies that can identify objects linked to an individual. However, the precise scope of the law and the intensity with which different use cases are regulated should depend on the available evidence about the context of the technology including the severity of risks associated with its use.

3.2. Automated Number Plate Recognition (ANPR) systems are already used effectively for law enforcement purposes, and there is currently a comprehensive legal framework governing their use (Home Office, 2024). Nevertheless, because ANPR does not involve biometric data or other similarly intrusive forms of data analysis, the new law should not include ANPR.

3.3. Clothing, vehicles (where not identified through plate numbers), and other objects are not unique identifiers, and there is currently no reliable evidence that existing technologies can accurately and consistently identify such objects in such a way that they are associated with an individual. There is a significant risk that objects are attributed to the wrong person due to similar or identical objects being possessed by several people.

3.4. Nevertheless, if object-identification technologies, can be shown to assist investigations more effectively than the task being carried out by police officers or persons, there may be a legitimate role for their use. Any such tools should be strictly limited to supporting human decision-making and should not be used as the sole basis for intervention. In practice, this would make their function comparable to a police officer visually identifying a vehicle, for instance.

3.5. At present, however, there is neither robust evidence of proven effectiveness nor a well-documented risk profile for these technologies. Before such tools are brought fully within operational use, a stronger evidence base is required to demonstrate both their reliability and their potential impacts.

3.6. The new law should create a basis for developing secondary laws that can ensure responsible use of such tools, when the need arises, and a strong case for their use is made. A principled and future-proof legal framework can achieve this.

4. Do you think that the types of technology the legal framework applies to should be flexible to allow for other technology types to be included in future? The alternative would be for Parliament to consider each new technology.

4.1. The new law should be flexible to include new similar technology use cases. An agile and future-proof legal framework is necessary to ensure that new use cases are subject to appropriate regulation, without parliament having to legislate whenever new similar technology use cases become relevant and appropriate for law enforcement.

4.2. Attempting to regulate a complex and rapidly evolving technology through a prescriptive legal framework risks producing regulatory ineffectiveness(unfitness): it may over-regulate certain use cases, under-regulate others, and create loopholes that cannot be effectively addressed in the absence of built-in mechanisms for adaptability(Asress Adimi Gikay, 2024). This aligns with the Government's overarching approach to AI regulation, which aims to introduce flexible, principles-based frameworks capable of being adapted and operationalised across different sectors rather than rigid and prescriptive rules that do not take into account the specific context of use cases(Asress Adimi Gikay, 2023b).

4.3. Generally, technology use cases that have similar functions, capabilities, and risk profiles should be subject to similar regulatory treatment. However, it is often difficult to produce an exhaustive or stable list of use cases that share similar capabilities and risk profiles, particularly in a rapidly evolving technological landscape (Asress Adimi Gikay, 2024). It is therefore more effective to establish a general principle within the legislation to allow for the inclusion of new, comparable technologies under the same framework, as the technology evolves.

4.4. At the same time, such a principled approach should prevent the law from over-fitting technologies that do not share relevant characteristics or risks or subjecting them to standards of general application that are not context-sensitive.

5. Do you think a new legal framework should only apply to law enforcement organisations' use of facial recognition and similar technologies for a law enforcement purpose?

5.1. The new law should apply only to law enforcement authorities.

5.2. The use of biometric technologies by private entities can be beneficial, but it also raises significant concerns, especially because many of the safeguards that apply to public authorities, such as equality impact assessment and other human rights considerations under the ECHR, do not apply to private sector deployers(Asress Adimi Gikay, 2023c).

5.3. Private entities should use such technologies in a compliant and responsible manner under existing data protection and other rules including the Surveillance Camera Code of Practice.

5.4. Until recently, the use of FRT by private entities such as retail businesses has been legally controversial, as biometric data generally cannot be processed on the basis of legitimate interest under the UK GDPR. Explicit consent as required by UK GDPR to process biometric data is difficult to obtain due to the infeasibility of securing such consent from customers on a mass scale on a daily basis in the context of LFR. In practice, businesses relied primarily on "substantial public interest" as a lawful basis under the Data Protection Act (DPA) 2018, which is interpreted narrowly, in other European jurisdictions with similar laws (Asress Adimi Gikay, 2023c); but such a narrow interpretation led to an effective ban on use of FRT by private entities in those jurisdictions.

5.5. The DPA 2018(Schedule 1(10)(1)) considers preventing or detecting unlawful acts as potential substantial public interest. However, the data processing in question must not be merely convenient but necessary to achieve substantial public interest(Asress Adimi Gikay, 2023c).

5.6. Retail businesses use FRT to effectively identify those on watchlists from engaging in shoplifting crimes using LFR or to identify suspected shoplifters by comparing biometric data using RFR. Shoplifting threatens safety of retail business employees, safety of the public at large and costs the economy (*see for* e.g., Eren Waitzman, 2024). As such using biometric technologies by retail businesses could be considered to serve substantial public interest, provided that the necessity to use the technology, rather than other tools is demonstrated.

5.7. The Data (Use and Access) Act (DUAA) 2025 explicitly recognises detecting or preventing crime to be a recognised legitimate interest under the UK GDPR (see DUAA, 2025 Schedule 2). This gives private actors a stronger legal position to use FRT, provided they comply with relevant UK GDPR obligations including data protection impact assessment and related obligations.

5.8. As the Information Commissioner's Office (ICO) also possesses clear enforcement powers over businesses, responsible use of FRT in the private sector can be ensured.

5.9. By contrast, the use of biometric technologies by law enforcement authorities is subject to a distinct legal regime, including Part 3 of the DPA 2018— the Law Enforcement Directive (LED). This separate framework reflects the unique powers and coercive authority of the state as well as the availability of large amount of data for the police that could potentially be misused.

5.10. There is no compelling reason that justifies removing the current separation of regulation and governance of biometric technologies as well as data protection law for law enforcement authorities and the private sector actors, even if the latter might use similar technologies for 'public safety' purposes.

5.11. Any attempt to combine the legal frameworks governing law enforcement and private entities would create unnecessary confusion and could result in inappropriate rules and standards being applied to one or the other regulated entity.

5.12. Other public sector organisations, such as local authorities, are subject to data protection regimes broadly equivalent to those applicable to private sector organisations and, as such, should also be excluded from the scope of the proposed law.

5.13. The processing of personal data by intelligence services is governed by the relevant Intelligence Services Data Protection Law (DPA 2018, Part 4), together with other relevant laws. These frameworks reflect the specific ways intelligence services operate, including the highly sensitive nature of their functions. Intelligence services also generally conduct covert operations, which fall outside the scope of this consultation. For these reasons, the new law should not apply to the use of biometric technologies, including FRT, by intelligence services.

6. When deciding on the new framework, the Government will use the factors listed above to assess how law enforcement organisations' use of biometric technologies, such as facial recognition, interferes with the public's right to privacy. What other factors do you think are relevant to consider when assessing interference with privacy?

6.1. There are important factors that are missing in the list leading to question 6 highlighted below.

6.2. Urgency / Immediacy of the Threat— Is there an imminent risk to life or public safety? Is delay likely to cause serious harm? This would be important in assessing interference with privacy rights, in particular proportionality.

6.3. The Inherent Intrusiveness of the Technology— Not all biometric technologies interfere with privacy equally. Emotion recognition systems are more intrusive as they involve inference of persons emotions and intents based on deeply personal behaviours such as smiles, facial expressions, sadness and voice tone. Comparatively, FRT does not involve intimate engagement with the subject being identified and therefore can be seen as relatively less intrusive. This is crucial in assessing interference with privacy rights and potentially determining the conditions and purposes for the permissibility of the use cases in question.

6.4. Accuracy and Reliability— The accuracy and scientific validity of some of the technologies is more tested (e.g., FRT) than others (e.g., emotion recognition or predictive AI). Legal standards should vary by considering these realities.

7. *****

8. Do you agree or disagree that 'seriousness' of harm should be a factor to decide how and when law enforcement organisations can acquire, retain, and use biometrics, facial recognition, and similar technology?

8.1. As a starting point, seriousness of harm is a good general framework to assess permissibility of various law enforcement AI tools. The Government's proposal also comprehensively lists factors that might be considered in assessing the seriousness of the harm including seriousness of the offence and number of offences.

8.2. One factor that should clearly be recognised under the seriousness-of-harm criterion is the seriousness of the offence involved. This factor should be used to determine whether certain deployments or uses are permitted. In particular, the new law should explicitly exclude non-serious offences from justifying the deployment of certain tools (e.g. LFR and RFR), with non-serious offences defined by the gravity of the applicable criminal penalty. This is necessary to maintain proportionality between the use of technology and the crime being investigated or the public safety threat being addressed.

8.3. Giving law enforcement authorities unlimited discretion in deploying biometric and inferential technologies for all types of crimes could lead to inefficient resource allocation, potentially shifting the focus from prioritising the quality of policing efforts to quantifying success based on the number of resolved crimes, no matter how petty the offences might be(Asress Adimi Gikay, 2023a).

8.4. To ensure the effective and responsible use of technology especially FRT, there needs to be a legal rule that establishes a clear requirement of non-deployment for certain offences. The rule should also contain an exception that allows law enforcement authorities to operate flexibly.

8.5. As biometric technologies such as LFR and RFR involve risks of engaging with mistakenly identified persons, sometimes leading to distressing interactions with citizens, subjecting deployments to a seriousness of offence threshold can lead to more conservative use and fewer instances of error as a result.

8.6. Excluding certain offences from warranting use of intrusive surveillance tools also aligns with public attitude, where support for biometric technology decreases with the decrease in the seriousness of the offences.

8.7. The Government's survey of 3,920 nationally representative respondents offers good insights into how the public views police use of LFR, RFR, and OIFR(Home Office 2025b). Overall, the public is broadly supportive of the use of FRT in policing; but support varies across demographic groups and gravity of the crimes.

8.8. At the highest end of severity, support is higher. RFR is considered acceptable by 91% of respondents for tackling terrorism, murder, and sexual violence while LFR enjoys similarly high support: 88–89% for terrorism and murder, and 87% for sexual violence as support remains strong for violent crimes causing injury (88% RFR, 84% LFR).

8.9. Support falls further where perceived physical(personal) harm is low (fraud: 62% RFR, 57% LFR and Antisocial behaviour: 61% RFR, only 56% LFR). This last figure indicates that the public might not view LFR as proportionate or necessary for low-level crimes.

8.10. The survey does not address public order offences. For instance, under section 4(A) of the Public Order Act 1986, intentional harassment, alarm or distress involves (a) using threatening, abusive or insulting words or behaviour, or disorderly behaviour, or (b) displaying any writing, sign or other visible representation which is threatening, abusive or insulting. It carries a maximum penalty of up to six months or a fine.

8.11. It would be difficult to justify scanning the faces of hundreds of thousands of people or searching against a national government database (biometric database that are not created for law enforcement purpose), to locate individuals suspected of such offences alone. The privacy intrusion, the risks of false identification and thus potentially engaging with an innocent person, and broader societal impact would outweigh the public safety benefit.

8.12. This does not mean that for instance LFR cannot be used in deployments where multiple serious offenders are on a watchlist. But low-level public order offences, on their own, would not justify an LFR deployment. Experience in other jurisdictions also suggests that it is politically questionable, especially when some public order offences such as harassing/insulting signs are held during non-violent political demonstrations. The prosecution of these offences can be politicised at times.

8.13. The ECtHR has held the deployment of LFR to target a protestor holding a placard in alleged violation of public order offence law to be unlawful because the technology was used to deal with an administrative offence which does not qualify under the Russian domestic law as criminal offence (*Glukhin vs Russia*, 2023). The deployment was considered to be in violation of privacy as well as freedom of expression.

8.14. The key take away from the reasoning was the failure of the deployment to meet both proportionality and legality elements under ECHR. In the UK, in Bridges, the Appellate Court found the deployment of LFR by South Wales Police unlawful because the applicable Standard Operating Procedure (SOP) gave police excessive discretion in determining who to put on the watchlist and where to deploy the technology ('the who and where questions').

8.15. If law enforcement authorities have the option of deploying LFR or using RFR to search a passport database for someone wanted for an offence punishable by six months or a fine, it is unlikely that the deployment addresses the "who" question that led to the finding of unlawfulness in Bridges.

8.16. As FRT continues to expand in policing, drawing clear proportionality boundaries is essential to preserve public trust. The proportionality requirement is in line with practice in other jurisdictions and aligns with the ECHR requirement of legality, which protects people from excessive police discretion in deciding for which crimes the technology can be deployed.

8.17. The exclusion of offences from justifying the use of biometric technology can still be nuanced. ***I propose a graduated proportionality rule for the new law set out in the proceeding paragraphs***.

8.18. To start with, certain crimes may not entail the required amount of imprisonment, but the frequency of their occurrence can have significant impact on society. A case in point is anti-social behaviours that involve damage to public property such as buses or threatening passengers and even disrupting transportation (see e.g., BBC, 2025).

8.19. In such cases, police might need to prioritise investigating the said crimes. Even if the general rule may exclude these types of offences from justifying the use of passport database for search using RFR, police can still use Police National Database (PND). As people whose images are in police-managed databases have provided them for law enforcement purposes, there is strong justification for searching such databases, with the risk to the rights of innocent people being relatively lower.

8.20. A second layer that can allow deployment is authorisation by the oversight body. In some cases, even if the offences are in principle excluded, the need to address such offences may justify the use of advanced technologies. In such cases, authorisation by an external(independent) authority may be necessary.

8.21. Finally, in the context of LFR, a legal requirement of proportionality can allow deployment for non-serious offences, if the watchlist at the same time targets serious offences.

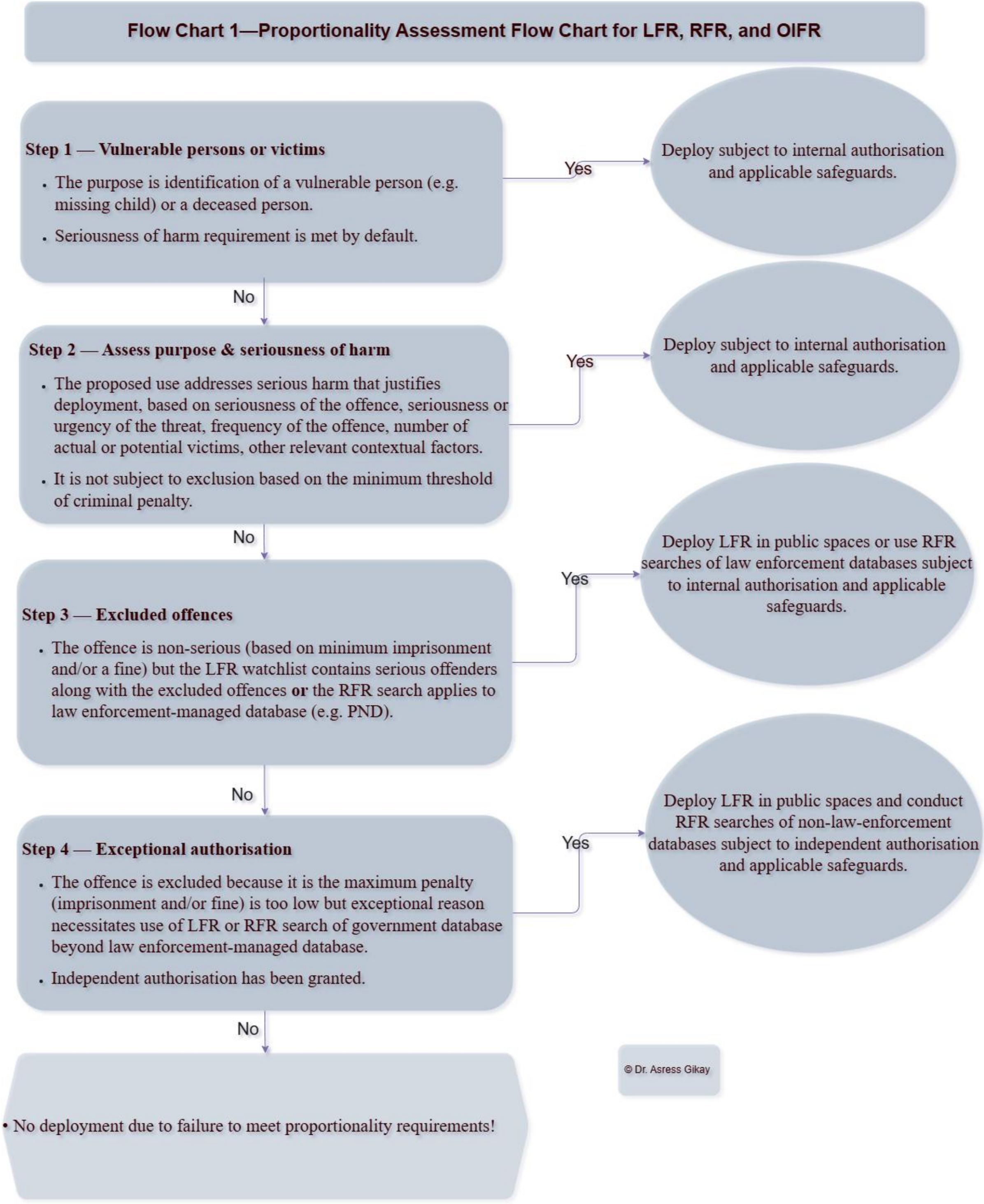
8.22. Based on the above, I propose four-pronged(graduated) proportionality assessment rules to be adopted by the new law as follows (visually presented in Flow Chart 1 below):

1. Vulnerable persons or victims carve-out— The use of FRT for the purpose of identifying vulnerable persons, such as missing children or deceased individuals, should not be subject to a seriousness-of-harm threshold. Such uses inherently involve serious harm and do not primarily raise risks for innocent third parties, as they do not involve potential direct attribution of criminal responsibility in most cases.

2. Seriousness of harm as the general gateway— In all other cases, the deployment of LFR, RFR, and comparable technologies should be justified only where the purpose of use is to address a serious harm. The seriousness of harm should be assessed by reference to factors including the seriousness of the offence, the seriousness or urgency of the threat, the frequency of the offence, the number of actual or potential victims, the nature of the victims and other relevant contextual considerations. The Governments' list of relevant factors is comprehensive in this regard subject to the caveat that it is always advisable to have a catchall phrase to allow for inclusion of factors that may be relevant but are left out.

3. Exclusion of non-serious offences with limited residual permissions— As a general rule, non-serious offences punishable by short terms of imprisonment and/or a fine should not, in themselves, justify the deployment of LFR in public spaces or the use of RFR to search non–law-enforcement databases, given the heightened risks this might pose to innocent people. However, law enforcement may still conduct RFR searches of law-enforcement-managed databases (such as the PND) or deploy LFR where the primary purpose of the operation is to address serious offences, and the inclusion of non-serious offences is ancillary to the primary objective.

4. Exceptional use subject to independent authorisation— Exceptionally, the use of LFR or RFR for otherwise excluded offences may be permitted where an exceptional justification exists and independent authorisation has been granted.



Flow Chart 1—Proportionality Assessment Flow Chart for LFR, RFR, and OIFR

Step 1 — Vulnerable persons or victims

- The purpose is identification of a vulnerable person (e.g. missing child) or a deceased person.
- Seriousness of harm requirement is met by default.

Yes → Deploy subject to internal authorisation and applicable safeguards.

No ↓

Step 2 — Assess purpose & seriousness of harm

- The proposed use addresses serious harm that justifies deployment, based on seriousness of the offence, seriousness or urgency of the threat, frequency of the offence, number of actual or potential victims, other relevant contextual factors.
- It is not subject to exclusion based on the minimum threshold of criminal penalty.

Yes → Deploy subject to internal authorisation and applicable safeguards.

No ↓

Step 3 — Excluded offences

- The offence is non-serious (based on minimum imprisonment and/or a fine) but the LFR watchlist contains serious offenders along with the excluded offences **or** the RFR search applies to law enforcement-managed database (e.g. PND).

Yes → Deploy LFR in public spaces or use RFR searches of law enforcement databases subject to internal authorisation and applicable safeguards.

No ↓

Step 4 — Exceptional authorisation

- The offence is excluded because it is the maximum penalty (imprisonment and/or fine) is too low but exceptional reason necessitates use of LFR or RFR search of government database beyond law enforcement-managed database.
- Independent authorisation has been granted.

Yes → Deploy LFR in public spaces and conduct RFR searches of non-law-enforcement databases subject to independent authorisation and applicable safeguards.

No ↓

- No deployment due to failure to meet proportionality requirements!

© Dr. Asress Gikay

9. What factors do you think are relevant to assessing ‘seriousness’ of harm? For example: the type of offence that has been committed; the number of offences that have been committed; the characteristics of the victim; whether there is an imminent threat to life, or there is an urgent safeguarding issue.

9.1. Factors relevant to assessing the 'seriousness' of harm include: the type of offence(*see response* to Question 8), number of offences (repeated or multiple offences can increase seriousness), characteristics of the victim(age, or special status may heighten harm), imminent nature of the threat to public safety or life or safety and the scale and impact of the harm including economic, social, or psychological consequences of the offence.

10. The Government believes that some uses of facial recognition and similar technologies require more senior authorisation and that this should be set out in the new legal framework. Do you agree? This could be different levels of authorisation within law enforcement organisations, or, in some circumstances, authorisation by a body independent of law enforcement organisations.

10.1. The current authorisation system, under which approval is provided by an officer of the rank of superintendent or above, is generally effective and there is no evidence that it is not functioning properly. Accordingly, there is no justification for replacing this system for most deployments. However, an independent authorisation mechanism should be introduced for certain limited use cases, i.e., for deployments involving excluded offences.

10.2. Additionally, to promote transparency and accountability, information relating to deployments should be made publicly available within a reasonable period after such deployments have taken place, so far as is practicable.

10.3. The proposed combination of internal and independent authorisation is in line with the recommended practices in other jurisdictions, mainly in the EU. The European Data Protection Board in its Guidelines 05/2022 on the use of FRT in the area of law enforcement recognises that internal authorisation could provide enhanced safeguards required in assessing the proportionality of interference with the claimant's right(EDPB, 2023). The EDPB stated in particular:

> The need for such safeguards is all the greater where personal data is subject to automatic processing and where there is a significant risk of unlawful access to the data. **Furthermore, internal or external, e.g. judicial, authorisation of the deployment of FRT may also contribute as safeguards and may prove to be necessary in certain cases of severe interference *[para 52]***.

10.4. Where a clear legal rule limiting deployment in respect of certain offences is in place, internal authorisation provides adequate safeguards while preserving efficiency and effectiveness in law enforcement operations. As noted earlier (*see* responses to Question 8), independent authorisation would nevertheless be required in certain circumstances, which are set out in the Authorisation Flow Chart 2(*see also* Paras 11.1-11.10).

11. Are there circumstances where law enforcement organisations should seek permission from an independent oversight body to be able to acquire, retain, or use

biometrics (e.g. use facial recognition technology)? This could include exceptional circumstances outside of the usual rules.

11.1. This question combines two distinct but related legal issues that should be considered separately.

11.2. The first is whether the deployment of technologies that acquire personal data including LFR, RFR, OIFR and potentially other biometric and inferential technologies should be subject to independent authorisation. The second issue is whether acquiring, retaining and using personal data requires authorisation. These are two separate issues, as the existing legal framework on these two issues are different.

11.3. Currently, data processing for law enforcement including obtaining, retaining, using and storage is regulated relatively adequately, although some clarity around data retention period is still necessary.

11.4. For example, LFR systems process personal data and may retain relevant data for a specific period depending on how the system is designed. However, the current practice already incorporates strong data protection and privacy by design and default features. In Metropolitan Police LFR deployments, biometric data acquired during deployment are deleted immediately or within 24 hours, while associated CCTV footage is retained for 31 days and automatically deleted without being accessed by a person(Metropolitan Police LFR Data Protection Impact Assessment, 2025). This adheres to the principle of storage limitation by design (or more generally data protection by design). Home Office's immigration LFR deployment document indicates even stronger safeguards, as scanning and comparing faces are conducted without retaining any footage(Home Office LFR Standard Operating Procedure, 2025).

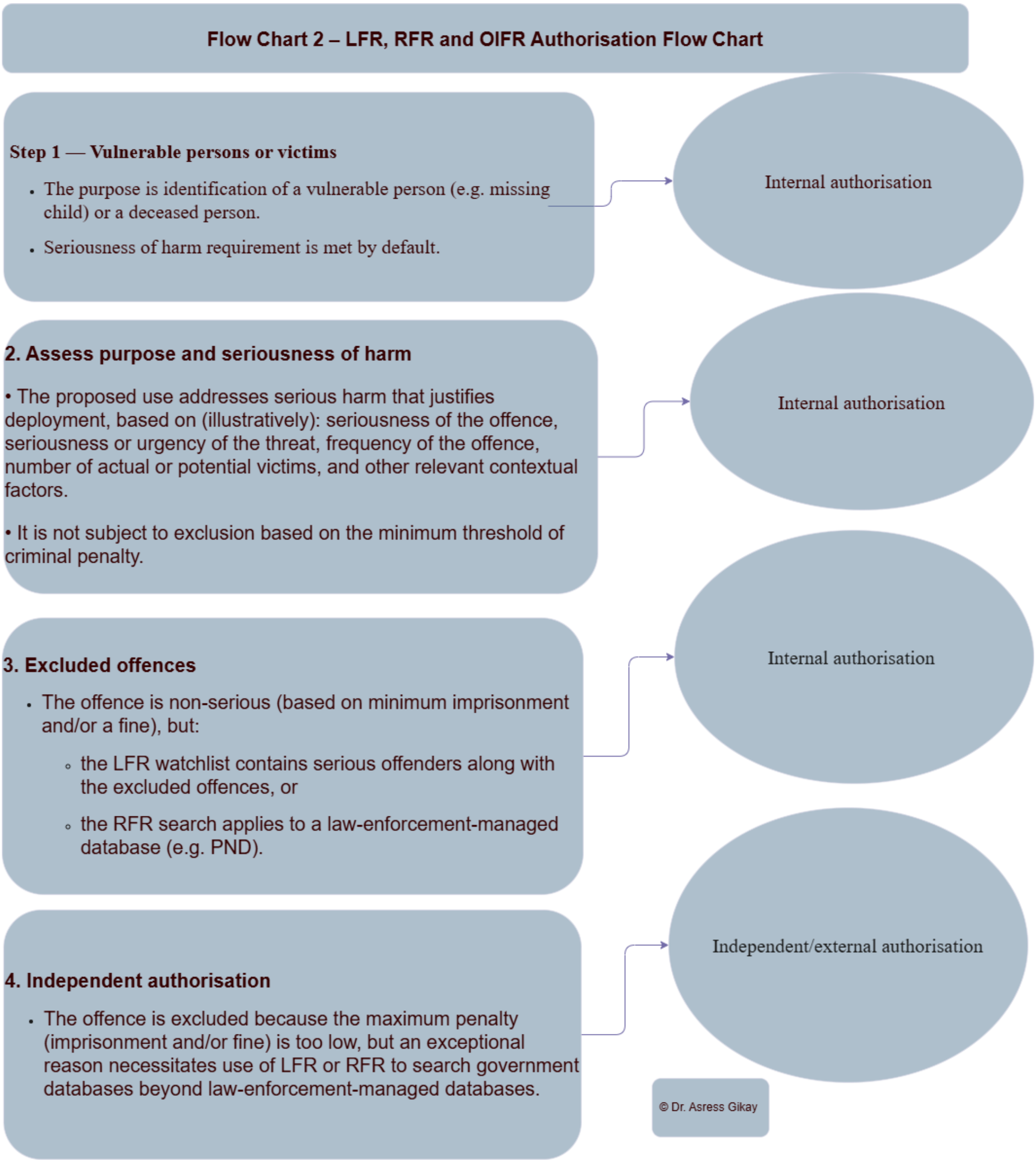
11.5. Data retention and use *per se* are not decisive factors in determining whether authorisation of deployment is necessary, although they are important factors. This is because as long as there is a lawful basis (law enforcement purpose), the current data protection rules provide adequate safeguards for data collection, use and retention.

11.6. In an LFR-based scenario, once a person is accurately identified and their image is retained for a lawful policing purpose (needed for further investigation), that retention is already governed by established data protection frameworks (including DPA 2018, Police Information and Records Management Code of Practice (MOPI) and related rules and policies). These regimes do not require specific authorisation for retention of personal data, and the ECtHR which had the opportunity to examine them in Catt vs UK (involving retention of the applicant's personal data including photos) has not considered lack of authorisation as a flaw in how they are designed. Instead, they are governed by the ECHR requirements of legality, necessity and proportionality. Therefore, currently, some biometric technologies should be subjected to authorisation, but not because of data use and retention as such.

11.7. As indicated earlier, the authorisation of certain uses of FRT and potentially other biometric technologies is necessary, not only because they process personal data but also because they involve other risks such as risks to freedom of expression and assembly as well as risks of bias and false identification. This requires a holistic view of authorisation that considers data protection as one element but also other issues including the overall proportionality of the specific deployment.

11.8. It is therefore necessary to introduce an independent authorisation mechanism for deployments that fall outside regular deployments, where such deployments do not meet the seriousness-of-offence threshold by default under the graduated serious harm analysis and law enforcement authorities must make a specific case as to why deployment remains necessary. In such cases, an independent body would assess whether the deployment should be permitted (*see paras* 12.1- 12.12 for details of the authorisation scheme for searches of government-database).

11.9. Independent authorisation becomes necessary where deployments or search of non-law enforcement database for excluded or non-serious offences is sought. This is primarily due to heightened risks to people's rights (such as freedom of expression and assembly), the potential for bias or false identification, the scale of privacy intrusion and the relatively lower public safety benefit. In such exceptional cases, law enforcement must make a specific, evidence-based case demonstrating necessity and proportionality, which should be scrutinised by an independent body to ensure that the use of biometric technology is justified considering the overall societal impacts.



Flow Chart 2 – LFR, RFR and OIFR Authorisation Flow Chart

Step 1 — Vulnerable persons or victims

- The purpose is identification of a vulnerable person (e.g. missing child) or a deceased person.
- Seriousness of harm requirement is met by default.

Internal authorisation

2. Assess purpose and seriousness of harm

• The proposed use addresses serious harm that justifies deployment, based on (illustratively): seriousness of the offence, seriousness or urgency of the threat, frequency of the offence, number of actual or potential victims, and other relevant contextual factors.

• It is not subject to exclusion based on the minimum threshold of criminal penalty.

Internal authorisation

3. Excluded offences

- The offence is non-serious (based on minimum imprisonment and/or a fine), but:
  - the LFR watchlist contains serious offenders along with the excluded offences, or
  - the RFR search applies to a law-enforcement-managed database (e.g. PND).

Internal authorisation

4. Independent authorisation

- The offence is excluded because the maximum penalty (imprisonment and/or fine) is too low, but an exceptional reason necessitates use of LFR or RFR to search government databases beyond law-enforcement-managed databases.

Independent/external authorisation

© Dr. Asress Gikay

12. If law enforcement organisations were not able to identify a person using law enforcement records and specific conditions were met, the systems could be enabled in such a way as to enable them to biometrically search other Government databases, such as the passport and immigration databases. In what circumstances should biometrics searches of other Government databases be permitted? (A) Searches should be for ‘serious offences. (B) Searches should be for a safeguarding purpose (e.g. a suspected missing or vulnerable person). (C) Searches should be to identify injured, unwell or deceased people.

12.1. Law enforcement should be permitted to search other government databases for all the above purposes using facial recognition. Nonetheless, limits and safeguards should apply as set out in the proceeding’s paragraphs.

12.2. *The new law adopts a three-tiered, risk-based framework for regulating police access to government databases, referred to as Category 1(high-risk), 2(medium risk)* *and 3(low risk)*. These categories are based on the purpose of the searches and the potential risks to the rights of innocent people who may be impacted by the facial recognition searches.

12.3. In Category 1(high-risk), law enforcement should seek independent authorisation to use FRT to search non-law enforcement government databases. This category consists of cases where it would be disproportionate to permit searches of sensitive databases for the investigation of less serious offences. Accordingly, in Category 1, given the potentially severe consequences of misidentification, offences that do not meet the seriousness-of-harm threshold by default should not justify recourse to intrusive investigative measures, unless specific case is made and an independent authorisation is granted.

12.4. In Category 2(medium risk), which concerns searches conducted in relation to serious offences, a seriousness-of-harm threshold applies. Where police are unable to locate perpetrators of serious crimes, such as murder, rape, or large-scale or serial fraud using police-managed databases alone, there is no principled justification for denying access to other government databases, including passport or immigration records. An interference with privacy right would be justifiable under the ECHR and other potential risks to the rights of other people should be considered tolerable, since there are safeguards that are followed in conducting such searches to mitigate harms to innocent people. For such searches, no independent authorisation would be required.

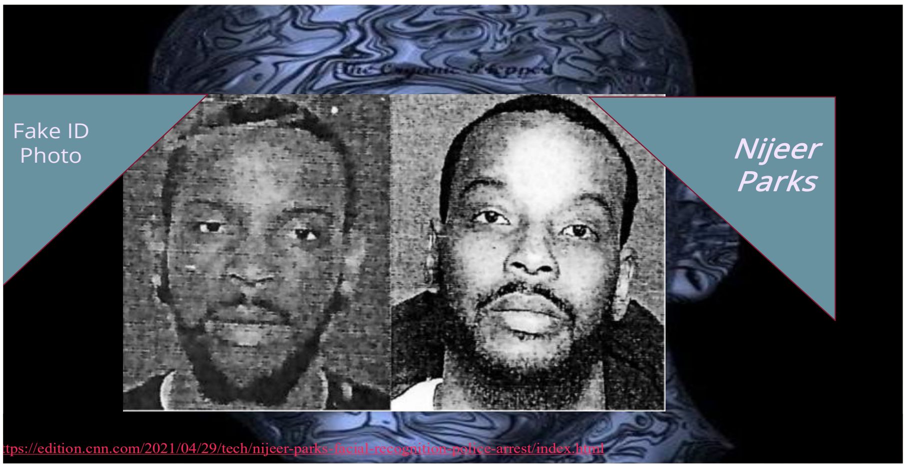
12.5. Category 3(low risk) covers searches conducted for protecting vulnerable persons (such as locating a suspected missing or vulnerable person) and searches undertaken to identify injured, unwell, or deceased persons. In these cases, the objective is to safeguard someone's right or wellbeing or to identify a potential victim. The risk of harm to others is minimal or non-existent, given that these searches do not entail allegations(imputations) of criminal conduct or the prospect of prosecution directly resulting from the searches. Imposing barriers on police access to databases in these circumstances would be unjustifiable, as it could hinder efforts to locate missing persons or to identify deceased individuals where no effective alternative means exist.

12.6. Regulating access to non-law enforcement databases based on risk category ensures that the use of advanced search technologies remains linked to the prevention of serious harm and is consistent with the principles of proportionality.

12.7. The risk-based approach considers previously documented risks to the rights of people, although this evidence is not related to UK law enforcement authorities' use of FRT. According to data from 2023, United States police have misidentified at least seven individuals using RFR, all of whom were Black(Katie Hawkinson, 2023). In several cases, those individuals spent time in custody before police acknowledged the false arrest.

12.8. Although UK police facial recognition systems are subject to rigorous testing, errors cannot be eliminated. This is evidenced by the most recent National Physical Laboratory testing of the Metropolitan Police Service's RFR system, which identified a significant disparity in accuracy rates across demographic groups, with Black women being significantly more likely to be misidentified(National Physical Laboratory Facial

Recognition(Cognitec) Equitability Report, 2025). In such circumstances, individuals may be exposed to substantial risks, including being required to prove their innocence, undermining the presumption of innocence. In some cases, these errors are difficult to avoid due to visual similarities between images.



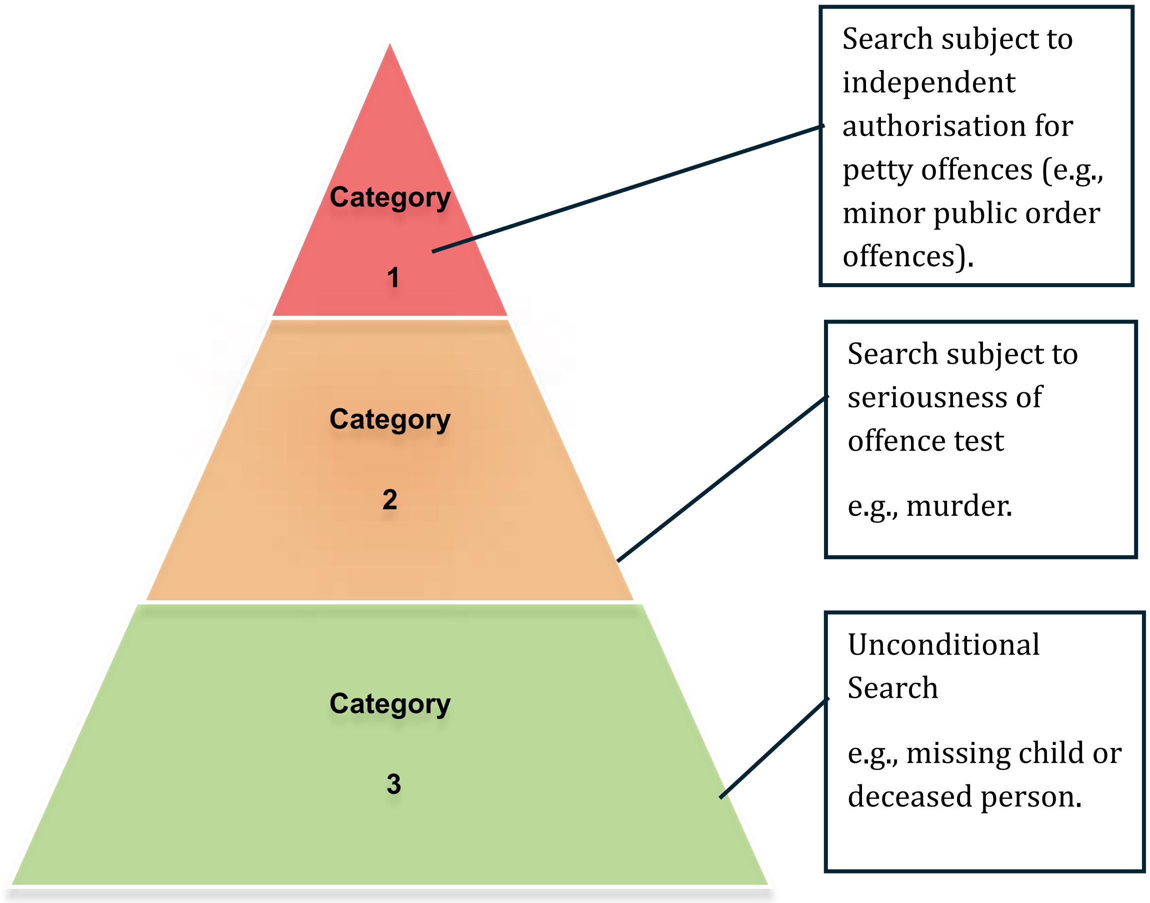
ttps://edition.cnn.com/2021/04/29/tech/nijeer-parks-facial-recognition-police-arrest/index.html

Photo Evidence 1: Comparison between a fake identification photograph recovered by police from a crime scene (left) and the genuine photograph of Nijeer Parks (right).

12.9. Nijeer Parks (in the photo above) spent 11 days in jail after being misidentified by Detroit Police using a crime-scene photograph compared with his photo in a police database. The civil rights lawsuit brought by the victim alleges serious abuses by investigating officers, triggered fundamentally by the false identification(Parks vs McCormac et. al, 2024). A seriousness threshold would help to avoid such incidents, when there is no urgency or over-riding public safety reason to identify the person in question urgently.

12.10. In all cases where search of government or law-enforcement databases is allowed, additional safeguards should be adopted including the requirement that any apparent match must be verified by at least two officers, with further verification required before an individual is treated as a suspect in the offence concerned (*see also* paras 13.1-13.4).

Facial Recognition Government Database Searches Risk/Permission Pyramid



Search subject to independent authorisation for petty offences (e.g., minor public order offences).

Search subject to seriousness of offence test

e.g., murder.

Unconditional Search

e.g., missing child or deceased person.

13. If biometric searches of other Government databases take place, what safeguards should be in place?

13.1. All biometric searches should be subject to approval by a senior officer. However, considering the need for heightened oversight in certain circumstances (*see paras* 12.1-12.11), some searches should require independent authorisation. This approach balances the need for the efficient deployment of biometric technologies in the investigation of serious offences with the need for enhanced safeguards where searches relate to less serious offences. While independent authorisation may cause some delays, such delays are justified where the risks to the public interest are comparatively lower. Delays can also be prevented by expedited authorisation or post-deployment authorisation in urgent cases.

13.2. In all cases, additional safeguards should be adopted including the requirement that any apparent match must be verified by at least two officers, with further verification required before an individual is treated as a suspect in the offence concerned.

13.3. This safeguard is consistent with the regulatory approach in the EU in respect of biometric technologies that qualify as high-risk AI systems. Article 14(5) of the (EU AI Act, 2025), which establishes requirements on human oversight, provides that no action or decision may be taken on the basis of the results of high-risk biometric identification systems unless those results have been separately verified and confirmed by at least two competent, trained and authorised natural persons, unless Union or national law considers the application of this requirement to be disproportionate in the context of law enforcement, migration, border control or asylum.

14. The functions set out above could be undertaken by one single independent oversight body – do you agree? This could be achieved by them overseeing multiple codes of practice (see also questions 15 and 16).

14.1. The functions set out by the new legal framework are appropriately undertaken by a single independent oversight body.

14.2. Biometric and inferential technologies present unique challenges. They raise issues of bias, inaccuracy, data protection and privacy, and engage multiple human rights, with the potential to cause compounded harms, i.e., harming multiple rights at the same time. They bring together areas that currently fall within the regulatory remit of different authorities, including the Biometric and Surveillance Camera Commissioner, the ICO, and potentially other regulators. None of these regulators are well-placed to regulate the use of these technologies by law enforcement authorities without jurisdictional overreach or leaving jurisdictional loopholes.

14.3. For instance, the ICO cannot regulate matters beyond data protection, such as algorithmic bias that engage equality law, except marginally through data protection impact assessment where risk of discrimination(bias) is one of the risks data protection impact assessments should address. Nor can it resolve disputes involving potentially unlawful deployment of these technologies where the unlawfulness relates, for example, to a failure to follow the required authorisation procedure.

14.4. Similarly, it would be inappropriate for the Biometric and Surveillance Camera Commissioner to assume jurisdiction over breaches of data protection legislation arising from the misuse of biometric technology by law enforcement authorities. This necessitates that any single effective regulator would need the authority to: (A) set standards, (B) enforce those standards, and (C) handle complaints, which may involve compliance with data protection law, authorisation requirements, and other laws including the Equality Act 2010.

14.5. If a new authority is not given the power to handle all relevant complaints through a **one-stop-shop**, the current confusion and fragmentation of oversight will continue. This would undermine the responsible use of biometric technologies, public accountability, public confidence, and equally importantly the rule of law.

14.6. Most complaints in relation to biometric technologies would likely involve data protection questions that fall under the ICO. This raises an important question: who would be the regulator when both data protection and other issues based on the new law are involved in a given complaint?

14.7. The proposed oversight body should be the lead regulator for all matters arising from the use of in-scope facial recognition and biometric technologies including: (1)

lawfulness of deployments, (2) compliance with authorisation and proportionality requirements, (3) technical standards relating to accuracy, reliability, and bias, (4) equality impact assessment and collective harms and (5) safeguards related to freedom of expression, assembly, and other relevant ECHR rights as well as all data protection issues that arise from the use of the in-scope technologies.

14.8. This does not mean the new regulator will be a data protection authority. The ICO should retain jurisdiction exclusively over stand-alone data protection matters that are primarily not related to the use of regulated biometric and other inferential technologies, such as general police data management practices, data security breaches, or the management of surveillance databases that do not implicate regulated technologies under the new law.

14.9. If both the new regulator and the ICO were given overlapping or undefined jurisdiction over complaints arising from deployment of biometric technologies, there would be several problems:

1. duplication of proceedings and inconsistent findings.
2. delay caused by jurisdictional disputes.
3. regulatory gaps where each authority defers to the other.
4. citizens being required to navigate multiple complaint systems.
5. declining public confidence due to institutional opacity.
6. decline in rule of law.

14.10. Embedding the new regulator within the ICO would risk over-burdening an already stretched regulator. At the same time, a new regulator without clear jurisdictional rules would generate precisely the fragmentation the new framework seeks to avoid.

14.11. The most coherent solution is subject-matter-based division of powers combined with a one-stop-shop public complaint model where all complaints arising from the use of in-scope biometric technologies are submitted to the new regulator as a single-entry point.

14.12. If a complaint involves any regulated deployment, it retains full jurisdiction, including on associated data protection issues arising from that deployment. Only where a complaint is purely a stand-alone data protection matter, with no connection to regulated technologies, is it mandatorily transferred to the ICO. The complainant should not be required to re-file the complaint as a single filing will be used by either regulator, and files will be digitally transferred to the ICO or vice-versa.

14.13. Under this model, new regulator applies its own statutory deployment and authorisation framework, the UK GDPR and the Data Protection Act 2018 and other relevant laws within a single, integrated decision-making process for mixed cases. These functions could appropriately be undertaken by a single independent oversight body.

14.14. The proposed model removes jurisdictional overreach and loopholes, prevents fragmentation, ensures legal certainty, and delivers an accessible one-stop-shop system of accountability and redress for the public.

15. What sort of powers or obligations should the oversight body have to oversee law enforcement use of facial recognition and similar technologies?

15.1. I agree with the powers listed in the Government's proposal. But the following should be added:

- Power to enter premises and access as well as inspect devices during investigations of potential violation of the regulatory rules.
- Power to issue warnings and reprimands to regulated entities.
- Responsibility to promote public awareness and education.

15.2. The above replicate the powers of ICO and there should not be a difference between the powers of the new authority and ICO in terms of overall aim and structure.

16. The Government believes the new oversight body should help set specific rules for law enforcement organisations to follow, to guard against bias and discrimination when using technologies such as facial recognition, and check compliance with these rules. To what extent do you agree or disagree?

16.1. I fully agree with the Government's proposal (see responses to question 14 and 15).

17. What types of rules might the new oversight body be responsible for setting? These could include ensuring tools are of sufficient quality or determining what testing should be undertaken.

17.1. The new oversight body should be empowered to set, maintain, and enforce technical and procedural standards grounded in recognised international norms. Centralising oversight would allow the regulator to mandate adoption of relevant ISO and IEC standards (for example, ISO/IEC standards on biometric performance, accuracy, robustness, bias testing, and information security), to require independent pre-deployment testing and periodic re-certification, and to issue binding codes of practice that translate those standards into operational requirements for law enforcement.

17.2. It could also accredit testing methodologies, approve audit frameworks, and require documented conformity assessments aligned with internationally accepted benchmarks, thereby ensuring consistency, interoperability, and technical rigour across deployments. By combining standard-setting, supervision, and enforcement within a single institution, the oversight body would reduce fragmentation, provide legal and technical certainty to police forces, and strengthen public confidence that biometric technologies are being used in accordance with objective, transparent, and internationally recognised standards.

Selected Bibliography

- Asress Adimi Gikay, ‘How the UK Is Getting AI Regulation Right’ *The Conversation* (8 June 2023) (Asress Adimi Gikay, 2023b).

- Asress Adimi Gikay, ‘Live Facial Recognition for Law Enforcement: The European Union’s Regulatory Approach Should be Informed by UK Police’s Practice’ (EU Law Analysis, 2023) (Asress Adim Gikay, 2023d).

- Asress Adimi Gikay, ‘Policing facial recognition is here to stay, risks included: What we need is a more honest debate’ The Register (18 September 2025).

- Asress Adimi Gikay, ‘Regulating the Use of Live Facial Recognition Technology by Law Enforcement Authorities: An Incremental Approach’ (2023) 82 Cambridge Law Journal 414(Asress Adimi Gikay, 2023a).

- Asress Adimi Gikay, ‘Risks, Innovation, and Adaptability in the UK’s Incrementalism versus the European Union’s Comprehensive Artificial Intelligence Regulation’ (2024) 32 *International Journal of Law and Information Technology* eaae013.

- Asress Adimi Gikay, ‘Using Live Facial Recognition to Tackle Retail Crime in the UK: What Does the Law Say?’ *Policing Insight* (7 August 2023) (Asress Adimi Gikay, 2023c).

- Home Office, *New Legal Framework for Law Enforcement Use of Biometrics, Facial Recognition and Similar Technologies: Government Consultation* (4 December 2025).

- Lena Podoletz ‘We have to talk about emotional AI and crime’ (2023) 38 AI & Society 1067, 1073.

- Matthew Ryder, The Ryder Review: Independent Legal Review of the Governance of Biometric Data in England and Wales (London, 2022), p. 8.

- Metropolitan Police Service, *‘Live Facial Recognition Annual Report’*, (September 30, 2025).

- National Physical Laboratory, *Accuracy and Equitability Evaluation of the Cognitec FaceVACS-DBScan ID v5.5 Facial Recognition Algorithm: Report for the Home Office and Office of the Police Chief Scientific Adviser* (October 2025).

- Pete Fussey and Daragh Murray, ‘Facial Recognition Surveillance: Policing in the Age of Artificial Intelligence’ (Oxford, 2025), p. 290.

- Rashida Richardson and others, ‘Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice’ (2019) 94 New York University Law Review Online 193, 195.