



To: fr-consultation@homeoffice.gov.uk

From: The Ministry of Ungentlemanly Warfare (Alt Productions)

Subject: Consultation response: New legal framework for law enforcement use of biometrics, facial recognition and similar technologies

Date: 24 January 2026

We submit this response to the Home Office consultation “New legal framework for law enforcement use of biometrics, facial recognition and similar technologies” (consultation period 04 December 2025 to 12 February 2026).

This response is written from a public-interest governance and evidence-handling perspective. We accept that law enforcement must have effective tools to prevent and detect serious harm, but we reject the normalisation of biometric mass-processing in public space as a default operating model. Any framework that makes such processing routine will predictably produce a structural shift in the relationship between citizen and state, where the public becomes continuously “checkable” without suspicion. That is not a minor policy change; it is a constitutional posture change.

We therefore recommend a framework that is deliberately restrictive, narrowly scoped, and enforceable in practice, not aspirational in guidance.

Executive position

The consultation recognises that facial recognition and adjacent biometric/inferential tools are “powerful” and raise legitimate concerns regarding privacy, oversight, public trust, and bias.

A framework that merely “clarifies” existing patchwork law while enabling significantly greater scale risks becoming an enabling statute rather than a protective one. The correct objective is not to expand usage safely; it is to define what must be *off-limits*, define what is *exceptional*, and force all routine use into lower-intrusion alternatives.

In plain terms, the legal framework should be designed to prevent “scale by default” and instead impose “exceptionality by design”.

Foundational principles the framework must hard-code

First, strict necessity must be treated as an operational threshold, not a rhetorical flourish. “Necessary” must mean that less intrusive methods are not reasonably available and have been exhausted, and that biometric processing is demonstrably outcome-critical rather than merely convenient.

Second, proportionality must be assessed against the predictable system-wide effect, not only the immediate policing objective. The consultation correctly notes that interference can affect individuals who are not subjects of investigation, and that factors include where and how data is acquired, whether overt/covert, the size of the

database/watchlist, and whether the biometric was acquired for another purpose (e.g. passports).

Those factors must become statutory gates with consequences, not optional considerations.

Third, the framework must explicitly protect democratic rights. The consultation itself flags the risk of chilling effects on expression and assembly, including protests and public gatherings.

Any regime that enables routine scanning around civic events will undermine public confidence in democratic participation even where no misuse is intended.

Fourth, the framework must treat function creep as a primary threat model. The consultation explicitly explores extending scope beyond facial recognition into inferential technologies (emotion, behaviour, suicidal intent) and object recognition tied to individuals.

This is not “future proofing”; it is building a legal runway for expansive surveillance modalities. The framework must resist scope expansion by default and require Parliamentary re-approval for materially new capability classes.

Scope: what technologies the framework should cover

Response to Questions 1–4 (biometric, inferential, object recognition, flexibility).

If a new statutory regime is created, it must cover any biometric technology that enables unique identification of an individual, because fragmentation will otherwise encourage regulatory arbitrage and capability substitution. We therefore agree that a framework should apply to biometric technologies used by law enforcement organisations for law enforcement purposes, but only if the framework is restrictive and includes enforceable safeguards with penalties and suppression remedies.

We do not support including inferential technologies (emotion, intent, behavioural inference) within the same enabling framework. The consultation’s examples explicitly contemplate inference at scale from CCTV feeds and behavioural signals.

These are categorically different from identification use cases because they move from “who is this person?” to “what is this person feeling/doing/likely to do?”, which pushes the state into predictive classification. If such technologies are contemplated at all, they should require separate legislation with a higher threshold, explicit prohibitions, and independent pre-authorisation. Treating inferential capability as merely another “technology type” is a governance error.

We also do not support bringing object recognition “linked to individuals” into a flexible enabling framework. While object recognition can be useful in retrospective investigations, its linkage to individuals at scale risks building behavioural trails and

association maps. If Parliament wishes to authorise this, it should be tightly limited to retrospective use with strict time windows, and with clear prohibitions on passive continuous tracking.

Finally, we oppose “flexible” scope expansion by secondary mechanisms. Question 4 proposes flexibility to include new technology types without Parliament considering each new technology.

We strongly disagree. Biometric and inferential surveillance capability is precisely the category where Parliament must make explicit, technology-specific decisions. “Flexibility” in this domain becomes a loophole.

Who the framework should apply to

Response to Question 5 (law enforcement only).

We agree the framework should apply to law enforcement organisations for law enforcement purposes, but we warn against creating a “gold standard” framework that inadvertently legitimises private-sector deployment by imitation. The consultation states that private/public sector users outside scope would still need to comply with UK GDPR/DPA 2018 with ICO oversight.

In practice, we have already seen in other domains that once government normalises a capability, commercial use accelerates and enforcement lags. The framework should therefore include an explicit statement of principle discouraging adoption outside law enforcement contexts and should mandate publication of best-practice constraints that the ICO can operationalise against non-policing deployments.

Privacy: what must be prohibited and what must be exceptional

Response to Questions 6–7 (additional factors for privacy and other rights interference).

The consultation lists factors for assessing privacy interference, including seriousness of harm, voluntariness, overt/covert nature, public/private space, intended subject status, access controls, whether used to locate/identify/infer, scale, and whether images were acquired for another purpose such as passports.

We agree with these and recommend the framework adds the following statutory factors:

The first additional factor is “baseline suspicion”. Live scanning of the public without suspicion is qualitatively different from scanning a suspect image from a crime scene. The law must explicitly distinguish “general population processing” from “investigative processing” and treat the former as presumptively unlawful except in tightly defined emergency conditions.

The second factor is “predictable chilling effect”. The framework should require an explicit assessment of whether deployment would reasonably deter lawful activity (attendance at protests, visits to sensitive locations, journalism, political association). This cannot remain a soft consideration; it must be a deployment-stopping gate.

The third factor is “misidentification cost”. The framework should require forces to quantify operationally what happens when the system is wrong: stop/search, arrest, use of force, detention, reputational harm, and downstream data retention. Proportionality analysis is meaningless if it ignores the harm profile of false matches.

The fourth factor is “data lineage and onward use”. If any data is retained, the framework must require strict limits on onward processing, cross-system enrichment, and secondary analytics. “We delete immediately if no match” is not a full answer if watchlist governance and match handling create persistent records elsewhere.

On other rights interference, the consultation highlights expression and peaceful assembly and the use of facial recognition at protests or on footage obtained at gatherings.

The framework must go further and establish an explicit prohibition on live facial recognition deployment at protests and political gatherings except where a judge has authorised it for a specific, serious, time-bounded threat, with strict minimisation, and with after-the-fact public reporting.

Seriousness threshold and permitted purposes

Response to Questions 8–9 (seriousness of harm).

We agree seriousness must be a factor. We recommend seriousness be operationalised into a tiered regime with statutory ceilings. In a democratic society, routine biometric scanning should not be permitted for low-level offences, convenience policing, or general deterrence. If the Government intends to permit “greater scale”, the seriousness threshold must rise accordingly, not fall.

We recommend the framework defines “qualifying offences” (as used in other biometric retention regimes) for live facial recognition and cross-database searching, and explicitly excludes minor offences. The seriousness assessment should also include the likelihood of necessity: where intelligence suggests a wanted person is not present, deployment is not justified.

Authorisation: who decides and what independence looks like

Response to Questions 10–11 (senior authorisation and independent approval).

We agree that some uses require more senior authorisation, but we do not believe internal authorisation alone is sufficient for high-interference deployments. An internal superintendent sign-off model is an administrative control, not independent oversight.

We recommend a two-track authorisation model. Routine retrospective use in a defined investigation can remain internally authorised under strict policy and audit. Any live facial recognition deployment in public spaces, any deployment near civic events, and any use involving cross-database biometric searching must require independent pre-authorisation by a judicial or quasi-judicial body, with a clearly defined test and the ability to refuse, amend, or impose conditions.

Question 11 asks about exceptional circumstances outside usual rules.

Our position is that “exceptional” must not become the operational backdoor. Exceptional authorisations should be limited to imminent threat to life or severe harm, and even then require immediate post-authorisation review, strict time limits, and public reporting after operational sensitivity passes.

Cross-database searching of passports/immigration and other records

Response to Questions 12–13 (biometric searching other Government databases and safeguards).

The consultation explicitly considers enabling law enforcement to biometrically search other Government databases, such as passport and immigration systems, under defined conditions.

This is the highest risk proposal in the document, because it creates a de facto national biometric identity search capability based on databases collected for other purposes.

We strongly oppose routine access. If such access is permitted at all, it must be constrained as follows: it must only be permitted for the gravest offences or immediate threats to life, it must require independent pre-authorisation, it must be time-bounded, and it must be subject to rigorous “last resort” evidence that all lower intrusion avenues have been exhausted, consistent with the consultation’s own published policy criteria describing public interest, likelihood of achieving aims, alternatives exhaustion, and proportionality.

On safeguards, we support senior approval, independent approval, and record keeping, but “record keeping” is meaningless without consequences. The framework must require auditable logs, mandatory periodic audits by an independent body, mandatory reporting of volume and outcomes, and suppression/exclusion consequences where searches were unlawful or non-compliant. It should also require accuracy and bias performance thresholds as a prerequisite for authorisation.

Oversight body: design it so it can actually stop misuse

Response to Questions 14–17 (single oversight body, powers, bias rules).

We accept the logic of consolidating oversight into a “one stop shop” provided it is genuinely independent, properly funded, and empowered to halt deployments. The consultation proposes an oversight body with powers including codes of practice,

investigation powers, compliance notices, injunctions, public declarations, complaint intake, and annual reporting, as well as standards for scientific validity and deciding which technologies should be added in future.

We support codes of practice and standards, but we do not support giving an oversight body unilateral power to expand the scope of the legal framework to new technologies. That is a Parliamentary function. The oversight body should advise and publish evidence; Parliament should decide.

For powers, the non-negotiable capabilities are: the ability to compel information, the ability to inspect systems and audits, the ability to issue binding compliance notices, and critically, the ability to obtain injunctions or otherwise stop deployments that are non-compliant or pose substantial risks. The oversight body must also be mandated to publish transparency reports, including aggregated statistics on deployments, false match rates, demographic performance differentials, and complaint outcomes.

On bias and discrimination, the consultation references equitability testing and public sector equality duties.

These should become statutory. The framework should require pre-deployment independent testing against relevant demographic groups, continuous monitoring, public reporting, and a duty to suspend use when performance degrades or disparities exceed thresholds.

Concrete statutory red lines we recommend

A workable legal framework must define explicit prohibitions, not merely principles.

Live facial recognition in public space should be prohibited as a routine tool and permitted only where a high seriousness threshold is met, where independent authorisation exists, where deployment is time and geography bounded, where watchlists are tightly governed, and where post-event transparency reporting occurs.

Use at or around protests, political gatherings, places of worship, healthcare facilities, and other sensitive contexts should be prohibited absent judicial authorisation for a specific and serious threat.

Inferential technologies (emotion, intent, behavioural classification) should be excluded from any enabling framework unless and until Parliament passes separate, explicit legislation with materially higher safeguards.

Cross-database searching of passports/immigration should not be normalised. If permitted, it must be treated as an extreme exceptional power, independently authorised, time-limited, auditable, and subject to enforceable consequences for misuse.

Closing position

The consultation is right that the public needs clarity and that law enforcement needs confidence.

But confidence should not be purchased by lowering the bar for biometric surveillance. The correct legislative outcome is one that makes the public confident that such technologies cannot silently expand into everyday life.

If the UK is to introduce a new legal framework, it should be designed as a constraint system that prevents mission creep, prevents bulk processing, prevents political chilling effects, and hard-codes independent oversight and meaningful remedies. Anything less will be interpreted, correctly, as the normalisation of population-scale biometric monitoring.

We request that the Home Office publishes, alongside its response, a plain-language “citizen impact statement” describing in concrete terms where and when a person may be biometrically scanned in public, what rights they have, how they can challenge misuse, and what consequences apply to unlawful use.

Respectfully submitted,

The Ministry of Ungentlemanly Warfare (Alt Productions)

Appendix: Historical Context, Constitutional Duty, and the United Kingdom's Democratic Inheritance

The Ministry of Ungentlemanly Warfare takes its name and ethos from a specific moment in British history: a period in which the United Kingdom confronted existential threat not by abandoning its values, but by defending them with clarity, restraint, and resolve.

The inspiration for the Ministry's framing is the legacy of unconventional but principled action taken during the Second World War, including operations such as Operation Postmaster, conducted under the direction and authority of the British state to resist the expansion of authoritarian power. These actions were undertaken not as expressions of unchecked state force, but as carefully bounded responses to an extraordinary threat, executed with a clear understanding of what the United Kingdom was defending: a free society governed by law, not fear.

Leadership during that period, including that of Winston Churchill, articulated a core principle that remains relevant today: that security and liberty are not opposing forces, and that the erosion of civil liberties in the name of safety ultimately undermines both. The defeat of authoritarian regimes in the twentieth century was not merely a military victory, but a moral and constitutional one.

It is from this lineage that our position arises.

We recognise the challenges facing modern law enforcement, including the need to address serious crime, public safety threats, and emerging forms of harm. We do not argue for technological stagnation, nor do we deny the potential utility of certain tools when deployed under strict, lawful, and proportionate conditions. Our concern is not the existence of technology, but the conditions under which it is normalised.

The United Kingdom's constitutional identity, under the Crown and Parliament, has historically rested on a commitment to individual liberty, due process, and the principle that state power must be constrained, reviewable, and accountable. These are not abstract ideals. They are the foundation of public trust, democratic legitimacy, and social cohesion. Any dilution of these principles, even incrementally and even with good intentions, carries long-term consequences that cannot easily be reversed.

In periods of heightened political, social, or geopolitical tension, there is a well-documented tendency for exceptional measures to become routine. History demonstrates that once intrusive powers are embedded into ordinary governance, they rarely contract; instead, they expand, adapt, and persist beyond the conditions that originally justified them. It is for this reason that safeguards must not merely exist on paper, but be structurally robust, legally enforceable, and resistant to erosion.

Our submission to this consultation is therefore grounded in a constructive objective: to assist in designing a framework that strengthens, rather than weakens, the United Kingdom's commitment to civil rights and civil liberties. The correct response to emerging technological capability is not to lower constitutional standards to accommodate it, but to raise governance standards to meet it.

A lawful and legitimate path forward lies not in broadening surveillance powers by default, but in reinforcing the United Kingdom's position as a jurisdiction that leads by example in the protection of fundamental rights while maintaining effective, targeted, and accountable law enforcement. That leadership, moral, legal, and constitutional, is part of this country's inheritance, and it remains one of its greatest strategic assets.

The only plausible and sustainable course is to strengthen civil liberties, reinforce fair and free justice, and ensure that any use of powerful technologies by the state remains firmly subordinate to the rights of the people it serves.