

Protecting Your Identity from Facial Recognition Systems

How face, eye, and head coverings affect automated identity recognition

How Facial Recognition Finds You

Facial recognition algorithms identify people by analyzing **key facial landmarks**. They measure features like the **distance between your eyes**, the **shape of your nose and jawline**, and the **contours of your eye sockets and eyebrows** ¹. The **eye region in particular (eyes, eyebrows, eyelids)** is crucial for matching faces ¹. Systems compare these unique facial characteristics to known images in a database, producing a **confidence score** for a potential match.

? What Makes You Recognisable

Distinctive facial features (especially around the eyes and brows) are critical for face recognition. Even if half your face is hidden, algorithms can often identify you by analyzing what's still visible.

FRT Evolves to Overcome Masks

Newer facial recognition algorithms have been **trained on masked faces** and show **high accuracy** on partially covered faces – sometimes under **5% error** on masked images. That's comparable to how well they performed on clear faces just a few years earlier.

[1](#) [2](#)

Coverings vs Recognition: Tiered Effectiveness

You can obscure your identity with **multiple layers: face coverings** (nose/mouth), **eye coverings** (eyes/eyebrows), and **head coverings** (hairline/forehead). Below we rank these measures by how much they typically **reduce facial recognition accuracy** in isolation (from minimal effect to greatest effect).

- **Face Coverings (mask, scarf over nose/mouth):**

Tier 1 – No mask: All features visible; *full* face recognition ability (ideal for

FRT).

Tier 2 – Partial cover (e.g., bandana below nose): Minimal effect because key landmarks (eyes, eyebrows, nose ridge) remain visible ¹.

Tier 3 – Standard mask (covers nose & mouth): Moderate impact; some algorithms can still identify masked faces with 95%+ accuracy ². Only lower face is hidden, so recognition success stays high.

Tier 4 – Full face cover (balaclava or veil): Maximum impact; most or all landmarks hidden. FRT accuracy drops dramatically ². Some systems may fail to find a face at all. (*This is effectively a mask plus eye cover combined.*)

- **Eye Coverings (glasses, sunglasses):**

Tier 1 – No eye cover: Eyes & brows fully visible; ideal conditions for FRT.

Tier 2 – Clear glasses: Negligible impact; transparent lenses don't hide eye features, so recognition stays ~unchanged ¹.

Tier 3 – Dark sunglasses: Medium impact; eyes hidden, forcing reliance on lower-face features. FRT accuracy declines (older systems saw error rates jump significantly) ¹. Still, with a mask *off* and only sunglasses on, algorithms often achieve decent matches using nose, mouth, and face shape.

Tier 4 – Opaque/reflective large sunglasses: High impact; eye region fully obscured, plus extra glare interference. This can considerably *increase error rates* (10× or more for some software) ¹. But note: if your mouth and nose are uncovered, algorithms still have plenty of data and can often identify you.

- **Head Coverings (hats, hoods, hair):**

Tier 1 – Hair & forehead visible: Full hairline and forehead shown; no hindrance to FRT.

Tier 2 – Small hat/beanie: Low impact; covers hair but leaves face and forehead visible. Face shape is still fully captured, so little accuracy change.

Tier 3 – Cap or brimmed hat: Medium impact; covers forehead and can cast shadows over eyebrows. FRT loses some context (face outline), causing more mismatches.

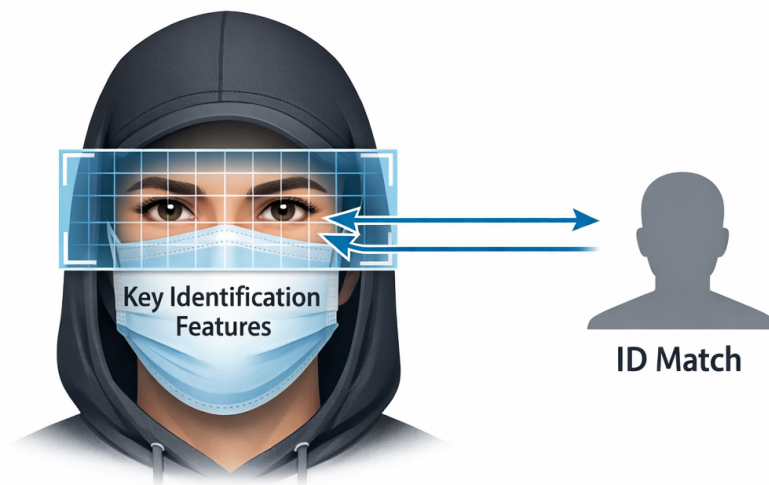
Tier 4 – Large hood or veil (with heavy shadow): Higher impact; hides forehead, hair, changes head shape silhouette. Alone, this confuses FRT somewhat, but not nearly as much as a mask or sunglasses do, because the core face is still unobstructed.



*Figure 1: Tiered coverage for identity protection. From left: **Tier 1** – no covering (full face visible, easy for FRT); **Tier 2** – standard mask only; **Tier 3** – dark sunglasses only; **Tier 4** – mask + sunglasses + hood (most features hidden, hardest for FRT). Partial coverings (Tier 2–3) still leave some unique features exposed.*

Why Partial Measures Often Fail

Covering just one part of your face (**mask without eye cover, or vice versa**) often isn't enough for anonymity. **Advanced FRT algorithms adjust** to whatever is visible. For example, with a mask on, an algorithm will hone in on your **eyes and eyebrows** to make a match ⁴. Even if half your face is hidden, an AI can compare the remaining half to your stored photos. The latest tests show many top systems can correctly identify a person wearing a typical COVID-style mask with only a slight accuracy drop ¹. **Sunglasses** also block eyes, but leave nose, mouth, and face shape visible – FRT can use those too.



*Figure 2: **Facial recognition finds visible features.** Even with a mask covering the nose and mouth, algorithms target the **eye region** (highlighted) to identify the person ¹. Partial coverings thus often fail to defeat FRT.*

Combining Coverings

Using **multiple coverings together (mask + sunglasses + hat/hood)** is **more effective** at confounding FRT than any single measure alone, because very few landmarks remain visible ⁴. This *layered approach (Tier 4)* can dramatically reduce automatic matching accuracy. **But** it may attract more attention from police or CCTV operators, since it's unusual in most contexts. Coverage beyond what's "normal" (like summer sunglasses or a winter scarf) may cause officers to watch or even stop you. They have on occasion singled out heavily covered individuals for photography or **stop-and-account** interactions (asking why you're covering your face) ⁴.

Legal Notes (UK)

In Britain, **it's generally legal to wear masks and coverings in public.** However, police have special powers in specific circumstances:

- **Section 60AA CJPOA 1994:** If police issue a **Section 60AA order** over a protest area, they can require you to **remove face coverings worn "wholly or mainly" to conceal identity** ⁴. Refusing a *direct request* to

remove a mask under such an order is a criminal offence, punishable by up to **1 month in jail or a £1,000 fine** ⁴. Police can also confiscate your mask ⁴. (They *cannot* normally demand removal without such an order, and they *should not* indiscriminately rip off masks – that could be assault ⁴.)

- **Human rights & necessity:** Under the **Human Rights Act 1998**, any police action (like forcing mask removal) must be **necessary and proportionate** (balancing **public safety vs your rights** to privacy, expression, and assembly) ⁴. Official guidance suggests that **face coverings shouldn't be banned in peaceful protests** unless there's a clear risk of imminent violence ⁴. Practically, however, police often justify Section 60AA orders by citing potential disorder.
- **Contextual use:** If you wear a covering for a non-identity reason (health, religion, cold weather, symbolic costume), that's not illegal ⁴. In fact, if charged under Section 60AA, proof that your face covering was mainly for a genuine reason (for example, a scarf for warmth or a COVID mask for health) can be a legal defence ⁴. Police judgment matters though – s.60AA depends on what officers *believe* your intent is, which can be subjective.

Privacy Trade-Offs

Covering your face in public for anonymity is a **trade-off between defeating technology and drawing attention**. More coverage **hampers facial recognition** but might cause police to focus on you for manual identification (like demanding your details or photographing you up close) ⁴. Conversely, less conspicuous measures (like common masks or sunglasses) won't stand out, *but* leave enough of your face visible for FRT to possibly recognise you ¹.

- If you're **especially worried about FRT (e.g. fear of doxxing or retribution)**, you might opt for stronger coverage. Just know the **legal boundaries** (e.g., you must remove coverings if lawfully ordered) ⁴.
- **Group context matters:** In a protest where many wear pandemic masks or sunglasses, **you blend into the crowd**, which might help. If you're one of few covering up heavily, you could ironically become **more memorable to observers**.
- **Supplementary tactics:** Consider combining physical measures with **other strategies**: avoid being isolated (stick with a group), be mindful of

where cameras are, and manage your **digital footprint** (avoid selfie or social media posts showing your face at protests).

Bottom line: No single mask or disguise guarantees anonymity. Facial recognition is improving rapidly and using multiple cues to identify people ². But **the more facial features you conceal, the harder you make it for an algorithm to recognize you.** Balance that with situational awareness: heavy cover can provoke police attention under certain conditions ⁴. Always prioritise your safety and be informed about your rights to protest and to privacy.