



Police, Phones & Your Rights: Biometrics vs Passwords (UK)

Protecting your phone is about understanding both **security** and **your legal rights**. These two things don't always line up in obvious ways, so this guide explains them clearly and simply.

Biometrics (Face ID, Fingerprint): What the Law Says

In the UK, police **cannot legally force you** to unlock your phone using:

- Your fingerprint
- Face ID
- Iris scan
- Any other biometric method

This is because using your body to unlock a device is treated as **self-incrimination**, which the law does not allow police to compel.

Important: While police cannot *legally* force biometric unlocking, someone could still try to **physically** use your fingerprint or face without your consent. That's why many security experts recommend turning biometrics off in situations where you may be at risk.

PINs and Passwords: What Police *Can* Compel

Although biometrics cannot be forced, police *can* legally require you to hand over your **PIN, password, or encryption key** — but only under a specific legal power:



Section 49 Notice (RIPA 2000)

Police must issue a formal notice requiring you to disclose your passcode. Refusing to comply is a criminal offence.

Penalties for refusing a Section 49 notice:

- Up to **2 years in prison**
- Up to **5 years** in national security or child indecency cases

You have the right to **legal advice** before responding.

So Which Is Safer — Biometrics or Passwords?

Here's the key point you need:

For legal protection:

Biometrics give you more protection because police cannot compel them.

For physical and personal safety:

A strong PIN or passphrase is safer because:

- Biometrics can be used against your will (e.g., someone forcing your finger onto a sensor)
- Biometrics cannot be changed if compromised
- A long PIN or passphrase is harder to bypass

The safest approach:

Turn off biometrics and rely on a strong PIN or passphrase. This gives you both:

- **Legal protection** (police cannot force biometrics)
- **Physical protection** (no one can unlock your phone by grabbing your hand or face)



Practical Tips for the Public

- Disable fingerprint and Face ID if you are concerned about privacy or police access.
- Use a strong PIN or passphrase (not 1234 or a simple pattern).
- If asked to unlock your phone, you can say: **“I do not consent to unlocking my device.”**
- If given a Section 49 notice, **seek legal advice immediately**.
- Keep your phone locked at all times — even short moments matter.

Helpful Resources

- **Liberty (UK Human Rights Organisation)** <https://www.libertyhumanrights.org.uk> Guidance on police powers and your rights.
- **Open Rights Group:** <https://www.openrightsgroup.org> . Digital rights, privacy, and surveillance information.
- **Big Brother Watch:** <https://bigbrotherwatch.org.uk> . Campaigns on police technology and civil liberties.
- **Law Society – Find a Solicitor:** <https://solicitors.lawsociety.org.uk> . For legal advice if you receive a Section 49 notice.