Argument against compulsory "BritCard" / Digital ID for all citizens

25 September 2025

I am firmly opposed to the introduction of a compulsory digital ID scheme for all British citizens (sometimes called "BritCard") as being proposed under Sir Keir Starmer's government. The idea may sound modern or efficient at first glance, but it raises deep issues of civil liberties, practicality, cost, and effectiveness. Below is my reasoning—and I believe many will share these concerns.

---

1. It represents a shift in the burden of proof — you become suspect by default

- Introducing mandatory ID for everyone treats all citizens as if they must *prove* their legitimacy. That's a reversal of the presumption that citizens already have the right to live, move, and engage in society freely.
- It signals distrust: rather than targeting those suspected of wrongdoing, the state demands universal surveillance or verification as a baseline.
- Even if the government says "only lawful residents will need it," once you normalize the infrastructure, scope creep is almost inevitable.
- The fact that there's already a petition demanding the government *not* to introduce a digital ID shows public unease. Petitions – UK Government and Parliament
- Civil liberties groups (for example Big Brother Watch) warn that "mandatory digital IDs give the state enormous control" and treat citizens with suspicion. The Independent+1

---

2. It is not the *form* of ID that fixes illegal immigration

- Police and immigration authorities *already* have legal powers to request identification in many circumstances (for example, under anti-social behaviour laws, during investigations, or at police stations). Citizens Advice+2GOV.UK+2
- If enforcement fails now, a new digital ID system will not magically change the political will, resourcing, or legal hurdles to arresting, detaining, deporting, or denying employment.
- The key is not whether an ID is digital or paper—it's *what happens* when someone is identified as undocumented. Without stronger enforcement or legal backing, a digital ID is a shell.
- Also, identity checks are one step; they must link to verification, consequences, and enforcement—if any of those links are weak, the system is toothless.

---

3. The cost, complexity, and risk are extremely high

- Rolling out a national digital ID system is a massive technological, administrative, and security undertaking. Mistakes will be made, delays will occur, and costs will balloon (as has happened with many large IT projects).
- Digital systems are targets for hacking, identity theft, cloning, data breaches, and misuse—introducing a centralized or widely used ID makes the stakes very high.
- If the database is compromised, lives, reputations, finances—all could be at risk. Even with best practices, no system is perfectly secure.
- Who controls the infrastructure? How is oversight, transparency, and accountability ensured? Who audits and with what legal recourse for individuals harmed?

4. Scope creep is almost inevitable

- Once the infrastructure is in place, political pressure will build to extend its use—to welfare, health services, travel, voting, public benefits, etc.
- What starts as “only for work checks or immigration control” can soon become a required credential to access everyday services.
- That centralization of power in identity systems is dangerous in any democracy.

---

5. It may actually push illegal migrants *further into the shadows*

- Civil liberties organisations warn that forcing mandatory identification could make vulnerable people more isolated—because those lacking valid ID will avoid all official systems and services, and rely on more hidden, unregulated environments. The Independent
- Migrants already stay off the grid when fearful of detection; a compulsory digital ID might heighten that fear.

---

6. Governments have tried before—and failed

- Britain had physical ID card proposals (under Tony Blair) which were abandoned amid cost, complexity, and civil liberties backlash.
- The current proposals face more advanced technology but also greater risks of overreach, privacy intrusion, and resistance.

7. Practicalities & fairness

- What about people who don’t have smartphones or reliable internet access? Not everyone can handle digital-only credentials.
- What about errors, mis-associations, identity disputes? If the wrong person is assigned or denied an ID, what recourse do they have?
- Would there be exemptions or appeals? How transparent would the system be?
- How do we ensure that it doesn’t exacerbate inequality (e.g. marginalized groups, the elderly, homeless) being excluded or unfairly burdened?

Ultimately, a digital ID does not fix the enforcement, legal, or policy failures we already have. It simply builds a modern infrastructure that could be exploited or misused.

A stronger alternative: focus civil and political energy on ensuring the system actually enforces the laws we have—funding border control, proper immigration adjudication, prosecuting employers hiring illegally, and strengthening removal mechanisms. Don’t demand a new identity regime instead of doing the job we already signed up for.

I call on Parliament, civil society, and fellow citizens: before we build sweeping identity control, demand accountability, transparency, restraint—and above all, preservation of our freedoms.

How does this fit with our Constitution?

Bottom line

- The UK has **no absolute constitutional prohibition** on mandatory ID cards. A future Act of Parliament **could** create them (Parliament is sovereign).
- However, our system builds in **serious friction**: common-law liberties,

Article 8 ECHR (privacy) via the Human Rights Act, and the **principle of legality** (Parliament must use clear words to curtail fundamental rights; vague wording isn't enough). Any ID scheme would face **privacy/proportionality tests** and political heat. UK Parliament+2lawprof.co+2

My instinct is rooted in our history

- Britain carried ID only as a **wartime emergency** (National Registration Act 1939); it was scrapped in **1952** after public backlash and concerns about police overuse (the **Willcock v Muckle** episode is emblematic). Wikipedia+1
- Labour's **Identity Cards Act 2006** set up a modern scheme but it was **repealed in 2010**; the database was destroyed. That's a recent, strong political precedent **against** national ID. Wikipedia

How an ID law would be tested

- **Article 8 (privacy)**: the state must show the scheme is **lawful, necessary and proportionate** to a legitimate aim (e.g., immigration control). If it's a dragnet or enables broad data sharing, it risks being found **disproportionate**. Courts won't strike it down outright (Parliament is sovereign), but could issue a **declaration of incompatibility**, creating immense political pressure. ECHR-KS+1
- **Principle of legality**: any attempt to use general wording to enable surveillance/repurposing would be read **narrowly**; **clear, explicit powers** are required to override basic rights. UK Parliament+1

There **is** a live **UK Parliament petition** "Do not introduce Digital ID cards." Citing that figure helps show democratic resistance. (Signature totals change rapidly; check the live page for the latest count.)

https://petition.parliament.uk/petitions/730194

Sign the Petition here.

What about the General Data Protection Regulations (GDPR)?

1️⃣ Lawful basis

- Every use of a digital ID must have a **lawful basis under Article 6 GDPR** (e.g. “legal obligation” if mandated by law, “public task” if used by government services).
- For sensitive categories (biometrics, race, health data) the bar is higher: **Article 9** requires explicit legal justification.
- That means Parliament would need to pass very clear enabling legislation spelling out exactly why and how data is processed.

2️⃣ Purpose limitation

- Data collected for one purpose (say, immigration checks) **cannot automatically be reused** for another (e.g. healthcare access, tax enforcement) without fresh legal cover.
- This directly curtails **scope creep** unless Parliament explicitly expands the law.

3️⃣ Data minimisation

- Only the **minimum necessary data** can be processed.
- So a digital ID shouldn’t include “everything about you” — just enough to verify identity. Holding extra details (address history, medical records, voting eligibility) risks breaching GDPR unless proportionate.

4 Transparency & rights of access

- Citizens must be told clearly how their ID data is used, who has access, and for what purpose.
- Individuals retain GDPR rights: **access**, **rectification**, **erasure** (where applicable), **restriction of processing**, and the right to complain to the ICO.

---

5 Security obligations

- Any centralised ID database would be classed as **high-risk processing**.
- Controllers must carry out **Data Protection Impact Assessments (DPIAs)** before launch.
- Strong technical safeguards (encryption, pseudonymisation, access controls) would be mandatory.
- Breaches must be reported to the ICO within **72 hours**.

---

6 Proportionality test

- Under GDPR and the UK Human Rights Act, any interference with privacy must be **necessary and proportionate** to a legitimate aim.
- If the system were too intrusive (e.g. tracking usage across multiple services), it could face a legal challenge as **disproportionate**.

---

7 Accountability & oversight

- The government (as data controller) must show **compliance with GDPR principles** at every stage.
- The **ICO** would oversee and could fine the government for breaches (though in practice, enforcement against government is politically fraught).

In summary:
A digital ID system *can* be made lawful under GDPR, but only with **clear legal basis, limited scope, and strong safeguards**. In practice, it would be hugely complex, constantly under legal challenge, and very costly to operate compliantly. That's why critics argue the system risks being both **expensive bureaucracy** and a **privacy liability**.