Written submission to the Home Affairs Committee's inquiry on "Harnessing the potential of new forms of digital ID"

Title:

Harnessing Digital ID? Evidence on eVisas, Share Codes, and Digital Immigration Status

Authors:

Dr Derya Ozkul, Dr Marie Godin, Sara Alsherif, Nazek Ramadan, Anne Stoltenberg, Daniel Sohege[i]

Introduction:

This submission draws on our collaborative research project funded by the ESRC Digital Good Network, "Digitising Identity: Navigating the Digital Immigration System and Migrant Experiences", a joint initiative between academic researchers Dr Derya Ozkul (University of Warwick/Oxford) and Dr Marie Godin (University of Leicester/Oxford), Open Rights Group (https://www.openrightsgroup.org), and Migrant Voice (https://www.migrantvoice.org).

Our project examined the introduction of eVisas and share codes for migrants to verify their immigration status.[ii] Here, we share some of our findings on how these new digital identity systems work in practice, and their impact on migrants' rights and daily life in the UK.

The UK government introduced the EU Settlement Scheme in 2018 to provide a mechanism to apply to to be demonstrate immigration status to EU, EEA, and Swiss citizens and their family members residing in the UK before Brexit. This marked the first instance of implementing an eVisa—a fully digital form of immigration status—as the sole proof of migrants' legal status. Despite many reported problems, the government has since extended the eVisa system to all migrants. Physical proof of immigration status became invalid by the end of December 2024 (later extended to June 2025), with migrants required to digitalise their status themselves.

Our research shows that migrants have effectively been used as test cases for digital ID systems, and their experiences reveal important lessons for policymakers.

Main problems identified:

- System errors and technical failures
- Inaccessible design
- Amplified burden of proof
- Exclusion from employment, housing and travel
- Lack of transparency
- No effective support or appeal process
- Erosion of trust and growing distress among migrants

Key recommendations:

- Prevent wider rollout
- Provide non-digital alternatives
- Extend transition periods
- Communicate clearly
- Offer in-person help
- Fix and simplify the share code system
- Prevent over-disclosure of data
- Design for everyone
- Create a timely appeal and redress mechanism
- Work together with and listen to users (in this case, migrants)
- Increase transparency

List of Questions:

How effectively is data relating to individuals currently being used and shared by the Home Office and its agencies?

The effectiveness of the Home Office's use and sharing of immigration-related data is not just about technical functionality, but also accuracy, transparency, security, and impact on the lives of individuals concerned.

Our research has shown that the current eVisa system is neither transparent nor accessible despite its goal to modernise the immigration system through digital infrastructures. Migrants face real risks of exclusion, discrimination and harm due to technical failures, unclear governance, and the increasing entanglement of immigration data with other public services.

Without significant reform—including strong legal safeguards, independent oversight, and transparent data governance—the system risks reinforcing inequality, increasing surveillance, and undermining trust in public institutions. Effective data use must centre not only on operational efficiency but also on fairness, accountability, transparency and respect for individuals' rights. Currently, the system does not meet these standards.

Our evidence shows that current data practices fall short in several critical areas:

Expansion of internal border controls and increased burden of proof

Migrants have described how digital status checks by third parties—particularly employers and landlords—often function as de facto immigration enforcement. We heard about system errors or incorrect status displays leading to migrants denied the rights afforded by their status, incl. employment or housing on that basis. Others described having to explain the digital system's operation—particularly the share code—to employers or landlords unfamiliar with digital status checks. These examples reflect a growing internalisation of border control, where everyday interactions are turned into immigration checkpoints with the burden of proof—and the cost of

system errors—falling disproportionately on migrants.

Lack of transparency and accountability regarding data sharing

There is no clear public guidance or oversight about how data held by the Home Office is shared with external actors. Particularly, how decisions are made about access, what safeguards are in place, and whether individuals are notified when their data is accessed or used by whom and for what purposes. This lack of transparency fuels anxiety and confusion among migrants. Many migrants are unsure who can view their data or how it may be used.

This opacity enables what is often referred to as "function creep," whereby a system originally intended to verify immigration status has expanded—without public scrutiny—into a general-purpose surveillance and enforcement tool. Notably, the eVisa system may be used to monitor individuals' movements in and out of the UK, and their interactions with various services provided by local authorities, along with universities, landlords, banks, and employers, amongst others.

The use of a cloud-based infrastructure for immigration data introduces further concerns about data security as it is not clear which third parties host or manage the data, how breaches are handled, or whether individuals have redress in cases of data loss, unauthorised access or misuse.

Technical failures

Migrants told us about various technical failures with the eVisa system, which have created new issues that did not occur with physical ID cards. It will sometimes display incorrect information, for example, indicating a 20-hour work limit despite the holder having a full-time work visa. In many instances, the system also froze or crashed during status verification processes, including in high-stakes situations like border crossings. These technical failures have both material and emotional consequences, including lost job opportunities, travel disruptions, and psychological stress. In some cases, individuals were left unable to prove their legal status despite having valid legal rights, such as indefinite leave to remain. Participants who called the Home Office's helpline about this had a long wait, and even then did not receive useful answers.

Lack of trust in public institutions

Without clear limits on how data is shared, or meaningful ways for individuals to challenge misuse or technical failures, the digital immigration status system risks reproducing and deepening a climate of distrust between users and public institutions.

What potential benefits could the use of new forms of government-issued digital identification have for the Government's ambitions to reduce crime and to manage migration?

The Home Office should carry out a comprehensive risk assessment comparing government-issued digital identification systems with physical card alternatives. This must include participatory consultation with migrants and assess data sharing practices, technical failure risks, and other potential harms. The review should be completed by the end of December 2025. To ensure transparency and enable public debate, the findings of the review should be published in full.

In particular, how could new forms of digital identification be used to:

i. Prevent and investigate crime, particularly fraud

The stated intention of digital identification systems is to enhance fraud prevention and investigative capacity, but without being designed with adequate safeguards, inaccurate or incomplete data, identity mismatches, and system integration errors can result in the wrongful identification of individuals, including innocent people being flagged as suspects. For digital immigration systems, these risks are particularly pronounced due to poor data quality.

Data collected for immigration or identification purposes may be repurposed for criminal investigations without appropriate legal oversight. Without strict statutory limits and independent governance, digital ID systems may enable forms of blanket surveillance, particularly affecting racialised migrant communities. Rather than preventing fraud, such practices risk eroding public trust.

ii. Manage border entries and exits

Digital identification systems, including the eVisa, are already being used at UK borders. Our research has shown a number of issues with these systems, including:

- Travellers are often denied entry to the UK or face significant delays due to technical faults, data mismatches, or system access problems.
- Digital records do not always reflect updated immigration statuses and travellers are unable to rectify errors at border crossings.
- Travellers are advised to keep their expired BRP cards, as they are considered more trusted than share codes.
- International carriers and foreign border authorities often do not always recognise UK digital-only documents; as a result, migrants may be questioned or delayed from boarding because eVisas are not deemed valid abroad. Consequently, some travellers are denied boarding and have to purchase new tickets.
- Finally, travel documents cannot be linked to eVisas, preventing those with refugee status from travelling outside the UK with full confidence.

Additionally, the Independent Monitoring Authority for the Citizens' Rights Agreements (IMA)

has raised concerns that the EU Settlement Scheme applicants holding a valid Certificate of Application face uncertainty and disruption when travelling due to conflicting Home Office guidance and inconsistent recognition by carriers and border officials.[iii]

iii. Support immigration enforcement

The use of digital identification to support immigration enforcement presents significant risks to the rights and safety of migrant communities. The errors we have seen in digital status records could lead to the threat of wrongful detention, removal, or denial of social services.

iv. Support labour market enforcement

Digital identification, as currently implemented through systems like the share code, is undermining rather than supporting labour market enforcement. Our research identifies multiple concerns with the share code system, including technical failures and a lack of awareness among some employers.

Migrants encountering problems with generating a share code, or with a share code displaying incorrect information about their right to work, face delays or exclusion from employment opportunities.

Employers are now expected to conduct immigration checks via digital systems that they often do not understand or are not aware of. Our participants reported having to explain the digital system to their (potential) employers. In this case, digital identification has shifted the burden of explaining onto migrants themselves.

v. Administer the asylum system

Digital-only identification models risk excluding those most in need of stability and protection. Without non-digital alternatives, accessible support, and safeguards tailored to vulnerable individuals, digital ID may deepen marginalisation rather than provide protection.

In the asylum system, the introduction of digital identification has amplified existing barriers to inclusion. Many refugees reported being unable to complete the digitalisation process for themselves or their children due to lack of internet connectivity, device incompatibility—particularly with older Android phones— or limited digital literacy. For some, interactions with the Home Office had already been so stressful that, when they did not receive official information about digitalising their status, they felt too overwhelmed to seek guidance online or navigate the Home Office's website.

Language and communication barriers compounded these difficulties. Instructions often found to be unclear, available only in English, and lacking adequate support, leaving refugees without the information they needed to complete the process.

A further technical issue involves the integration of travel documents with the eVisa system. Refugees with travel document issued from the UK could not link their passports to their digital status, creating a serious risk of being stranded abroad or denied re-entry to the UK. In one case, a refugee participant on a temporary visa had to travel abroad without any clear guidance from the Home Office, despite repeatedly requesting assistance. The only response they received from the Home Office was that travelling would be at their own risk.

Would government-issued digital identification need to be mandatory to realise these benefits?

The mandatory digital-only immigration system was introduced without essential safeguards. It was rolled out without a published Data Protection Impact Assessment (DPIA) and without any non-digital alternatives. Our Freedom of Information requests to access the DPIA were refused. By making digital status compulsory for all migrants, the system leaves those unable to use it without a way to prove their legal status. In effect, migrants have been made test subjects for a mandatory digital identification scheme—implemented without proper oversight, consultation, or avenues for redress.

Digital identification cannot be presumed to deliver benefits unless those benefits are deliberately and equitably built into its design. At present, the UK's digital immigration infrastructure has not met its stated goals of efficiency, security, and reliability. Instead, it has deepened inequality, created new forms of precarity and exclusion, and undermined the basic rights of migrants.

The system disproportionately harms those with limited digital literacy, without advanced smartphones, laptops, or stable internet connections. Many participants reported that older devices, especially Android models, were incompatible with the application process. Others could not complete the process for themselves or their children due to hardware limitations, poor connectivity, or difficulty taking photos because of the system's rigid design. Those without the required technology need to borrow someone else's device, opening them up to exploitation and abuse.

Barriers are even greater for people with disabilities, caring responsibilities, and families with multiple dependents. The eVisa system is particularly inadequate for children and adults with disabilities—for example, families with severely autistic children were unable to complete photo verification and thus could not digitalise their children's status.

Home Office communications often compound these problems. Migrants described them as confusing, inconsistent and sometimes inaccessible—especially for people with limited English. Some did not receive notifications, while others in the same household did, creating further confusion and stress.

The lack of clear, trusted guidance from the Home Office has created space for misinformation

to spread via social media. Participants reported exploitation by private solicitors charging excessive fees to complete what is meant to be a free process. Out of desperation, some participants turned to online groups—exposing themselves to inaccurate information and potential financial exploitation.

Accessibility, transparency, and accountability must be prioritised before any expansion or continuation of mandatory digital identification systems.

What different categories of information about individuals could most usefully be included in government-issued digital identification?

Government-issued digital identification should adhere strictly to the principle of data minimisation, as provided by Article 5(1)(c) of UK GDPR. Only the information that is strictly necessary for the specific function being performed should be included and visible. Government-issued digital ID should not display sensitive personal data to non-governmental entities unless there is a clearly defined legal and functional justification. The default should always be the minimum necessary information for the task at hand.

Findings from our research show that the current digital immigration system frequently discloses more information than necessary to users, and at times, this is inaccurate information. For example, refugee status labels are shown to employers, even when only the right-to-work is relevant. This over-disclosure, our participants believed, has led to job refusals and stigmatising treatment.

What implications would the inclusion of different categories of information have for the efficacy of digital identification for law enforcement and/or immigration enforcement purposes?

For law enforcement and immigration compliance purposes, efficacy depends not on the quantity of data included in digital IDs, but on:

- Accuracy: ensuring that status data is correct and current;
- Redress: ensuring the ability to rectify or update inaccurate information promptly;
- Granularity controls: limiting who sees what data, based on need and legal authority;
- Auditability: tracking who accessed which data, and for what purpose, with respect for data protection and privacy
- Clear boundaries between social service provision and enforcement functions.

Without these safeguards, any operational benefits from data-sharing are outweighed by systemic errors, rights violations, and loss of public trust.

What potential risks does the adoption of new forms of digital identification have for individuals, including risks to privacy and security of personal data?

While this question highlights privacy and data security, our research findings indicate that migrants often rightly perceive other risks as more pressing—particularly exclusion from services, loss of income or housing, inability to travel, and the risk of discrimination. These experiences are deeply connected to technical design flaws, lack of transparency, and weak governance of the digital ID system, all of which compromise privacy and security as well. Findings from our research reveal how these risks manifest in practice for those subject to the UK's digital immigration infrastructure.

Overall, the adoption of digital ID systems—without robust safeguards—poses multiple risks:

- Loss of individual privacy through over-disclosure and data sharing without consent;
- Insecurity, financial losses and emotional distress caused by technical errors and lack of recourse;
- Discrimination, exclusion, and harm from system failures.

What capabilities would the Home Office and its agencies need to develop to effectively introduce and take advantage of new forms of digital identification?

Our research with migrants shows systemic flaws in the current digital-only immigration status system. There are important lessons to be learnt before any broader digital identification systems are considered.

Our recommendations to the Home Office, based on our research, are:

1. **Prevent wider rollout and provide non-digital alternatives, such as physical identification.** Do not make digital systems compulsory. Where documentation is needed, people need ways to show their status that do not depend on smartphones, internet access, or digital skills.

2. **Extend transition periods.** Both migrants and other end users need time to understand, adjust, and make their choices regarding the digitalisation process.

3. **Communicate clearly.** Use simple, multilingual, accessible communication about digital ID. Provide clear information as to what individuals can do when they reach technical glitches.

4. **Offer in-person help.** People need more support services for digital ID than for physical ID systems. We need in-person support services from the government and trusted community organisations for people who struggle to use online systems. The current Home Office hotline is not fit for purpose.

5. **Fix and simplify the share code system and inform end users** (eg landlords, employers, flight staff and border officers) so that migrants are not denied services they are eligible

for based on a lack of understanding about digital systems.

6. **Prevent the over-disclosure of data**. The eVisa system must be updated to only show the data needed for the purpose.

7. **Design for everyone.** Build systems that work for those with low levels of digital literacy, people with no access to compatible devices, and people with disabilities.

8. **Create a timely appeal and redress mechanism**. Set up fast, transparent ways to appeal errors, and make sure migrants and end users know how to use them.

9. **Work together with and listen to users (in this case, migrants)**. Many of these issues could have been addressed from the outset if migrants' experiences were built into the process of designing digital ID systems.

10. **Increase transparency.** Clearly set out who can access immigration data, for what purposes, and with what safeguards.

How can the Government learn from the use of new forms of digital identification work internationally?

A robust public dialogue about the purpose, design, and governance of such systems must precede any move towards the expansion of digital identification systems in the UK. It is essential to ensure that individual rights are protected and that no one loses access to services or legal entitlements due to a poorly designed and unfair digital ID system.

[i] Dr Derya Ozkul is an Assistant Professor at the University of Warwick's Department of Sociology and a Research Associate at the University of Oxford's Refugee Studies Centre (RSC). Dr Marie Godin is an Assistant Professor in Human Geography at the University of Leicester's School of Geography, Geology and the Environment, and a Research Associate at the University of Oxford's Centre on Migration, Policy and Society (COMPAS). Sara Alsherif is the Migrant Digital Justice Programme Manager at the Open Rights Group. Nazek Ramadan is the Director, Anne Stoltenberg is the Head of Development, and Daniel Sohege
is the Advocacy and Communications Manager at Migrant Voice.

[ii] This research is based on 40 in-depth interviews with migrants holding various legal statuses in the UK and two roundtables at Migrant Voice's office in London involving migrant-led charities and organisations. This research is funded by the ESRC Digital Good Network through the University of Sheffield (Grant Reference: ES/X502352/1).

[iii] IMA. 2025. IMA raises concerns about travel difficulties for EU Settlement Scheme applicants, 11.08.2025, https://ima-citizensrights.org.uk/news_events/ima-raises-concerns-about-travel-difficulties-for-eu-settlement-scheme-applicants/