OpenVoiceNews U.K.

Transparent. Unbiased. Yours.

Biometric Technology Paves the Way for Digital ID Transition and Expanded Credential Use

August 3, 2025

— Categories: Breaking News

Download IPFS

Biometric systems are rapidly transforming identity verification, replacing traditional, outdated forms of identification with secure, adaptable digital formats. As governments and institutions look to streamline public services, travel, and online safety, biometric credentials are playing a central role in updating legacy systems. This week's top

developments in biometrics highlight a global shift toward modern digital ID solutions, the expansion of digital wallets, and concerns surrounding security, privacy, and implementation.

The United Kingdom is making a significant change to its post-Brexit passport program by ending its contract early with French defence and tech firm Thales, which previously won the deal amid political controversy. The UK Home Office has begun the tender process for a new contract, reportedly worth up to $533 million, that includes Digital Travel Credentials (DTCs) as part of Biometric Travel Documents for visas and immigration services. The update aligns with the broader trend toward integrated digital identities.

Within the UK's domestic system, the Department for Work and Pensions aims to double the user base of its One Login single sign-on (SSO) platform. There is also ongoing discussion of a new national ID card dubbed the "BritCard," although concerns have been raised about potential rising costs. These efforts signal a government-wide initiative to unify and expand digital identity infrastructure.

Nepal's Supreme Court has cleared the government to proceed with new contracts for biometric passports with German firms Mühlbauer and Veridos. The decision follows a legal challenge by Idemia Smart Identity over alleged procurement irregularities. The Court determined that the claims did not justify halting the agreements, allowing Nepal to move forward with its digital ID modernisation.

Europe's long-anticipated Entry/Exit System (EES), which will replace manual passport stamping with biometric checks using facial recognition and fingerprints, is scheduled to be fully implemented by April 2026. The phased rollout begins in October 2025 and is expected to overhaul border management across the European Union.

In the Asia-Pacific region, New Zealand has issued a request for proposals (RFP) to develop a platform for issuing digital credentials into the government's Digital Wallet. The platform is expected to support a wide range of credentials, including DTCs, and be delivered as a managed service. This comes shortly after the country selected providers for its Government App and wallet infrastructure.

Ethiopia's digital transformation continues to progress, with 900 public services now accessible online through the national digital ID system, Fayda, and the MESOB platform. Connectivity challenges remain, but telcos and the Ministry of Innovation and Technology

are working to improve interoperability and infrastructure under the nation's digital public infrastructure (DPI) strategy.

Canada has faced challenges with cyber insurance as municipalities transition to digital systems. The city of Hamilton, Ontario, was denied a CA$5 million (US$3.6 million) claim following a cyberattack, due to the absence of strong credentials and multi-factor authentication (MFA). The case underscores the importance of robust security protocols in digital government services.

In the United States, facial recognition technology is being expanded at airports by the Transportation Security Administration (TSA), aiming to reduce reliance on physical passports. However, a report by the Algorithmic Justice League raises concerns about informed consent and treatment of those who opt out. The report claims some travellers face mockery or verbal abuse when declining biometric screening. A small group of U.S. lawmakers is also seeking to halt the TSA's use of facial recognition.

Simultaneously, federal surveillance programs are drawing criticism. Immigration and Customs Enforcement (ICE) has come under scrutiny for its growing use of ankle bracelets in tracking individuals. Meanwhile, a $128 million contract has been awarded to defence contractor Leidos to expand the FBI's Next Generation Identification (NGI) biometric and criminal history database.

On the local level, New Orleans has introduced a municipal ID card designed with privacy protections. The card enables residents to access city services without risking exposure to immigration enforcement, reflecting a cautious approach to the use of biometric and digital IDs.

Digital ID systems are increasingly used not to identify individuals directly, but to confirm specific attributes such as age. Following the UK's enforcement of the Online Safety Act (OSA), platforms like Yoti, an identity verification provider, have seen a significant spike in usage. The rise in age verification tools has also prompted an increase in VPN usage, although the Age Verification Providers Association (AVPA) notes that the law lacks clarity on accountability for content accessed via VPNs. The group also challenges the notion that minors unintentionally download VPNs to access adult content.

Concerns about overreach in age gating were further stirred when indie game platform Itch removed titles containing adult content. The platform claimed it took action to avoid

pressure from payment processors Stripe and PayPal, reportedly influenced by activist group Collective Shout.

The continued evolution of biometric and digital ID technologies is reshaping how governments, businesses, and individuals approach identity, security, and access. As this transformation unfolds, issues of privacy, transparency, and accountability will remain central to public debate and policy decisions.