The Expose

expose-news.com Printed on January 26, 2026

UK government is designing and installing a Digital Identity Panopticon

January 25, 2026

By her own admission, the UK Home Secretary, Shabana Mahmood, aims to create a digital identity Panopticon using AI and technology to constantly monitor citizens.

The UK government's digital identity system will use biometric data, such as facial recognition, to create unique identity tokens, enabling real-time monitoring and predictive analysis of individual behaviour.

To establish the official UK digital identity Panopticon, the government and its partners do not require us to adopt any new forms of digital identity. Though it is trying to manipulate us into submitting our biometric authentication token to its GOV.UK digital identity wallet. And once we are manipulated into adopting our digital identities, they will be made interoperable across the whole of the UK economy.

Let's not lose touch…Your Government and Big Tech are actively trying to censor the information reported by The Exposé to serve their own needs. Subscribe to our emails now to make sure you receive the latest uncensored news in your inbox…

Stay Updated!

Stay connected with News updates by Email

Enter your name

Enter your email

ARE YOU A HUMAN? 6 + 3 =

Join Us

The Official UK Digital Identity Panopticon

By Iain Davis, 24 January 2026

Chatting with former UK Prime Minister Tony Blair in December 2025, UK Home Secretary Shabana Mahmood said:

> y ultimate vision for that part of the criminal justice system was to achieve, by means of AI and technology, what Jeremy Bentham tried to do with his Panopticon. That is that the eyes of the state can be on you at all times. we've already been rolling out live facial recognition technology, but I think there's big space here for being able to harness the power of AI and tech to get ahead of the criminals, frankly, which is what we're trying to do.

The UK Home Secretary has ministerial responsibility for the Home Office portfolio. The Home Office's purported intention is to "to keep citizens safe and the country secure." In truth, as revealed by Mahmood, the Home Office is currently part of a public-private state that is attacking us to protect itself.

Though the official UK digital identity Panopticon will supposedly only target criminals, in order to identify them, from among millions of British citizens, the state will spy on everybody all of the time.

To be clear: The UK government's official position is to use AI as the "eyes of the state" and to set its gaze firmly "on you at all times." This is the openly stated purpose of the official UK digital identity Panopticon.

Jeremy Bentham's proposed Panopticon was a circular prison with a central observation post, or watchtower, that could potentially see into every cell. Unsure if they were being watched, the theoretical prisoner was compelled to behave as ordered at all times. The envisaged Panopticon oppression stemmed largely from self-regulation.

The official UK digital identity Panopticon goes much further than Bentham could have possibly imagined. As its prisoners, there will be no reason for us to harbour any doubts. We can be certain that we will be under constant surveillance. Unlike the 18th century model, the modern AI-based digital Panopticon will not rely on self-regulation, though that socially engineered condition will still persist.

Mahmood claims the state's Panopticon objective is to identify criminal behaviour. Of course, what the state determines to be criminal behaviour is liable to change.

For example, the newly expanded state definition of extremism determines that intolerance – meaning to reject the idea – of the UK's "system of liberal parliamentary democracy and democratic rights" is extremist.

Despite there being no evidence to support its view, the UK state further asserts: "Extremism can lead to the radicalisation of individuals and can lead to acts of terrorism. he government committed 'to challenge extremist ideology that leads to violence, but also that which leads to wider problems in society'."

Peaceful, law-abiding citizens who question if Parliament is actually the "supreme legislative authority with the ability to make or unmake any law" are among the many who represent "wider problems in society." As we've just highlighted, if, as it says, it has the authority to make or unmake any law, the state reserves the right to define any behaviour as criminal at any time.

Those of us who question the state are far from alone in having reasons for concern. Even the most loyal subjects are targeted.

When Mahmood announced that the government was trying to "harness the power of AI and tech to get ahead of the criminals," she was alluding to law enforcement initiatives like Project Nectar. The police have piloted the use of commercial analytics software – Palantir Foundry – to supposedly predict when we might be "about to commit a crime." This averred predictive capability is based on some AI assessment of our digital identity-generated risk signal.

With legislation like the Terrorism Prevention and Investigation Measures Act and the Counter-Terrorism and Security Act already on the statute books, the government's glare is staring us in the face. Say the wrong thing online, express the wrong opinion or pose the wrong question and, using our digital identities, any one of us could find ourselves subject to AI-dictated reprisals, including incarceration without trial.

As things stand, the biometric data – facial recognition images – of 45 million British passport holders and, overlapping that number, 55 million drivers, are set to form the biometric authentication tokens that will single out our individual digital identities within the envisaged digital identity data lakes.

AI can then use our identity token to isolate our individual behavioural patterns, detect anomalies, and predict whatever the state deems to be a risk associated with our behaviour. The real-time speed of AI pattern recognition enables the constant monitoring of our activity. The state can then deploy AI to execute predetermined conditional smart contracts to instantly restrict or withhold our access to goods and services – or worse.

The state will have possession of the ultimate tool for socially engineering our individual behaviours and, consequently, the whole population. An Agentic State – a state ruled by the autonomous, automatic decisions of AI – can be formed and a full-blown Technocracy imposed.

Please watch this short video outlining the true nature of digital identity in the UK.

The Official UK Digital Identity Panopticon

The Official UK Digital Identity Panopticon, 21 January 2026 (9 mins)

If you are unable to watch the video above on Rumble, you can watch it on Odysee HERE. You can watch the whole discussion HERE. Ant Critchley's Becoming Stellify. Support Ant Critchley's work. Watch on Odysee.

According to the UK state, "An identity is a combination of 'attributes' (characteristics) that belong to a person. A single attribute is not usually enough to tell one person apart from another, but a combination of attributes might be."

The government has established the UK Digital Identity and Attributes Trust Framework ("DIATF") to ensure those of us "who want or need a digital identity" are issued one. This is an illusory Hobson's choice.

The only way to access any government services will be by using digital identity. Whether we "want" one or not, we will "need" a state-approved digital identity to obtain a marriage certificate, file a tax return (a legal requirement where applicable), apply for a driving license, rent or buy a home, or register for health care, etc. The UK government calls this evident necessity "optional."

The DIATF is overseen by Government Digital Services ("GDS"), which is part of the Department for Science, Innovation and Technology ("DSIT"). Josh Simons MP is the Parliamentary Under-Secretary of State for DSIT. He is also a leading parliamentary spokesperson and lobbyist for Labour Growth Group PLC. As such, Simons' objective is to tear down the barriers to economic growth by pushing bold and practical reforms on behalf of multinational corporations.

The Trilateralist Keir Starmer, a close associate of fellow Trilateralist Larry Fink – the BlackRock CEO and co-chair of the WEF – appointed Simons as the "minister for digital reform in charge of spearheading the government's digital ID plans."

On the 15th January, Simons told Parliament that the purpose of digital identity policy was to "transform the state," by controlling our "access services across both the public and private sectors." Simons assured parliament and the British people:

> Digital IDs will be rolled out for free to everyone who wants one. If anyone does not want one, they do not have to have one. ccess to public services will not be conditional on having . The Prime Minister has been clear on that, and I can underscore that commitment.

As usual, there is a vast chasm between ministerial statements and their verbal commitments and the reality of the public-private state's actions. For a start, the rollout of the UK's official digital identity Panopticon is not "free."

The cost to the UK taxpayer of the digital transformation of our health and social care sector alone is set to eclipse £21 billion. This represents a direct transfer of wealth from the people (the public sector) to global corporations (the private sector). Multinationals such as Palantir and Oracle profit from the digital infrastructure contracts to "transform the state." Using the Government to enable corporate profiteering from the public purse is the primary objective of Labour Growth Group PLC.

If, as Simons claims, we will not need to use our allocated digital identities to access public services, then alternative non-digital pathways should be provided. None are currently planned or even proposed, so this element of Simons' parliamentary statement wasn't true either. It is hard to see why those of us who decide to reject digital identity should pay tax for government services we can't use.

For example, UK company directors are being compelled to verify their identities online, using the UK government's One-Login portal, to retain directorship registration. There are two ways they can avail themselves of this government service.

They can either register their biometric digital identity token directly with the state or "verify" themselves through a third party – an Authorised Corporate Service Provider (ACSP) or via the Post Office. But, whichever route directors use, their digital identity authentication token is created and they are cast into the official UK digital identity Panopticon. Their only realistic option is not to comply.

As part of the planned Panopticon, the UK government is moving swiftly towards forcing us to use our designated digital identities to access the internet. With regard to restricting our ability to share information online, state mouthpieces have been dispatched to convince us that banning under-16s from using social media has something to do with child safeguarding. Obviously, this is another paper-thin lie.

To verify our age on social media platforms, every one of us will need to use a digital identity. The UK state has already legislated to extend this likely requirement beyond social media, soon to control our access to the entire internet.

The Data (Use and Access) Act 2025 ("DUAA") establishes a national framework for the digital identity verification of individuals to use online public and private services. It contains some very reasonable online protections for children. This ensures that anyone who opposes the dictatorship lurking within it can be cast by state propagandists as a risk to children.

Despite the fact that the UK supposedly left the EU in 2016, the DUAA has incorporated the EU legal concept of an "information society service" ("ISS") within its sledgehammer diktats. An ISS is the kind of amorphous legal construct that can easily be interpreted via secondary legislation – which is precisely what the DUAA proposes – to mean whatever the state wants it to mean.

Wrestling with this ambiguity, the UK Information Commissioner's Office ("ICO") has interpreted what an ISS implies in the context of the DUAA. It notes that an ISS "is not restricted to services specifically directed at children," and further determines that an ISS is: "ny service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services."

The ICO adds:

> Essentially this means that most online services are ISS, including apps, programs and many websites including search engines, social media platforms, online messaging or internet-based voice telephony services, online marketplaces, content streaming services (e.g. video, music or gaming services), online games, news or educational websites, and any websites offering other goods or services to users over the internet.

It is blatantly transparent that the services we pay for from an Internet Service Provider ("ISP") – the means by which we access the internet – is an "information society service" for the purposes of the DUAA. We will inevitably need "highly effective age verification" – digital identity – to use the internet in the UK.

The Digital Identity and Attributes Trust Framework ("DIATF") establishes the "technical and operating standards for use across the UK's economy." The goal is to achieve "international and domestic interoperability" of all digital identity-based products and services – across both the public and the private sector.

The state claims this is essential because the "digital transformation of the global economy" is accelerating. Therefore, "a digital identity to prove your right to work in the UK" can also be used to "open a bank account." This necessitates public-private partnership and the sharing of digital identity data "across the UK economy."

Interoperability means our **enforced** digital identities will be "built and operated in a standardised way." Software such as Palantir Gotham – incorporating Palantir Foundry – can take data from any source, such as your state-issued driving license, your privately issued bank card, or your police record, to "visualise and analyse information from multiple systems in real time across the operating environment to achieve successful mission outcomes."

The UK state has a strategic partnership with Palantir. It provides Palantir Gotham and Foundry to government departments and agencies – evidently including the police – through its current G-Cloud 14 procurement programme. Gotham and Foundry are among the UK government's "AI-driven analytics tools."

Once we are manipulated into adopting our digital identities, they will be made interoperable across the whole of the UK economy. This means that the state will be able to "produce actionable intelligence based on the full ecosystem of available data."

To establish the official UK digital identity Panopticon, the government and its partners do not require us to adopt any new forms of digital identity. Though it is trying to manipulate us into submitting our biometric authentication token to its GOV.UK digital identity wallet – for the public-private state, this is just the most expedient method of imprisoning us in its Panopticon.

If we refuse be corralled via One Login into the GOV.UK prison wallet, the state merely has to ensure the digital identity system we already use, nearly every day, is interoperable to achieve the same ends. Once interoperability between so-called "vendor agnostic" digital products and services is established, the government and its propagandists simply need to convince us to keep using them.

As the network of live facial recognition technology expands across the UK, combined with our allocated interoperable digital identities, everything we buy, every service we use, everywhere we go, every person we meet, every aspect of our lives – our health, insurance and financial data, etc. – will be monitored, tracked and recorded in real time. Thereafter, using AI, restrictions can be placed on our permitted behaviour in real time.

This will be our shared reality if we continue to use the digital identity system that has already been built in the UK by successive governments and their partners.

The UK state currently utilises deception, coercion and force to rule us. Once it has established its Agentic State Technocracy it will have total behavioural control of its citizenry and won't need to rely so heavily on deceit and intimidation.

The official UK digital identity Panopticon is being constructed and it will be controlled by a UK public-private state dictatorship. The state has already passed legislation to control our access to information online, to censor our freedom of speech and expression, to remove our supposedly democratic right to protest, and has granted to itself and its agents immunity from prosecution for any crime.

Our right to annul legislation – to render it legally invalid – through trial by jury has been a seldom-used but firm part of our constitutional landscape for hundreds of years. Not only is the UK state severely restricting our lawful right to trial by jury, its so-called judges now claim they have the unconstitutional power to punish juries if they annul.

The Court of Appeal ruling to that effect is, at best, erroneous and appears to be completely unlawful. Unfortunately, those of us who still cling to the notion that the UK functional oligarchy – the public-private state – and its Establishment henchmen and women have any interest in observing our constitutional rule of law are hopelessly deluded.

The only real choice any of us have is stark.

Irrespective of whether we submit to the government's new digital infrastructure – One Login and the GOV.UK wallet – those of us who continue to use the products and services currently available to us will be, in all likelihood, imprisoned within the UK state's official digital identity Panopticon. Our only chance, in the short term, is to refuse to comply with pretty much the whole digital system.

We must reject these extant systems, throw away our smartphones, refuse to use government online portals, decline private sector services that require our digital identity as a prerequisite, and actively pursue and adopt possible alternative networks.

We have no choice but to use every peaceable and lawful means at our disposal to defend ourselves against the UK state.

About the Author

Iain Davis is an autodidact, a journalist, an author and a researcher. He is the creator of the blog IainDavis.com, formerly known as '*In This Together*'. He publishes articles on his Substack page, *Unlimited Hangout*, *Geopolitics & Empire*, *Bitcoin Magazine* and other outlets.

You can pre-order his upcoming book '*The Technocratic Dark State*', HERE and listen to a discussion about the book HERE.

Featured image taken from 'What does the panopticon mean in the age of digital surveillance?' The Guardian, 23 July 2013

The Expose Urgently Needs Your Help…

Support the Expose

Can you please help to keep the lights on with The Expose's honest, reliable, powerful and truthful journalism?

Your Government & Big Tech organisations try to silence & shut down The Expose.

So we need your help to ensure we can continue to bring you the facts the mainstream refuses to.

The government does not fund us to publish lies and propaganda on their behalf like the Mainstream Media.

Instead, we rely solely on your support. So please support us in our efforts to bring you honest, reliable, investigative journalism today. It's secure, quick and easy.

Please choose your preferred method below to show your support.

Monthly Subscription

Monthly Donation

One-Time Donation

Buy us a Coffee

Stay Updated!

Stay connected with News updates by Email

Enter your name

Enter your email

DAILY DIGEST
US NEWS POSTS
UK NEWS POSTS
WORLD NEWS POSTS
ALL NEWS POSTS

ARE YOU A HUMAN? 1 + 8 =

Join Us

Forgotten Heroes: Edith Cavell

Davos 2026 Unpacked: What Was It Really About?

Climate change: Davos got off on the wrong foot

Why the Black Death is so important to the pandemic industry