

Joint Statement

4 October 2025

CIJ, A19 & Sinar Project Have Concerns About E-KYC

The Centre for Independent Journalism, ARTICLE 19 and Sinar Project are deeply concerned about the recent [announcement](#) by Malaysia's Minister of Communications, Fahmi Fadzil, that all social media platforms operating in Malaysia will be required to adopt a mandatory electronic Know-Your-Customer (e-KYC) verification using government-issued documents, such as MyKad, passports, and MyDigital ID, when the [Online Safety Act \(ONSA\)](#) comes into effect at the end of 2025 or early 2026.

While the Malaysian government has a legitimate interest in addressing the issue of online scams, fraud, and protecting children from harm, we must also recognise that the proposed initiative raises significant implications for the protection and promotion of the right to privacy, freedom of expression, and digital inclusion. We are already witnessing a trend where the government is amending or introducing new legislation that expands the powers of the Malaysian Communications and Multimedia Commission (MCMC), yet enforcement of these regulations lacks transparency and independent oversight. The risk of abuse and selective enforcement is high, with growing evidence of targeted suppression or arbitrary takedowns.

We urge the government and regulators to halt any hasty imposition of e-KYC mandates on social media platforms and to carefully consider how the issue of online scams, fraud, and protecting children from harm can be addressed in a manner that does not threaten human rights. This must include meaningful consultations with human rights

organisations and civil society. Otherwise, this move carries the risk of further eroding rights within digital spaces in our country, including by concentrating powers over identity systems in ways that are difficult to undo.

We must also stand together to avoid a situation where, once established, the e-KYC infrastructure may expand beyond social media (e.g. forums, news comment sections, messaging apps), ultimately intensifying centralised government control of our digital space. Such a function and scope creep will erode public trust in digital governance and the integrity of Malaysia's online ecosystem.

Key Concerns

1. Privacy and data protection risks

Malaysia's current legal landscape does not provide a robust safeguard and necessary protection in terms of privacy and data protection. The collection and storage of highly sensitive personal identity data (MyKad, passport, and other digital identification) at such a scale would have a high possibility of breaches, misuse or leaks.

In this context, requiring social media platforms to collect and store sensitive personal identity information would increase the risk of data breaches and cyberattacks. . Data breaches are not uncommon in Malaysia, and the country has already experienced repeated [data leaks](#), including from government-linked databases. Mandating e-KYC under such conditions not only exposes users to heightened privacy, surveillance and security risks, but also undermines public trust in digital platforms.

Surveillance and data privacy are closely linked issues, with significant human rights implications for individuals and society. Implementing e-KYC will entail tying account activity to real identification and metadata (IP addresses, devices, timestamps). This

infrastructure could enable more intrusive monitoring of online behaviour (e.g., information about who comments on which posts and interacts with whom and even inferred attributes such as emotions or political beliefs), whether by state actors or through compelled cooperation with platforms.

Even if no illegal activity takes place, such information can be used to develop profiles, anticipate behaviour, or stifle criticism.

When paired with algorithmic systems that assess the visibility of posts or assesses when they go viral assess advertising, and risk scores for law enforcement, such surveillance can amplify algorithmic bias, resulting in the discriminatory profiling of communities at risk, activists, or other marginalised or vulnerable groups. This threatens to reproduce and reinforce systemic and entrenched inequalities disguised as digital “safety.”

2. Chilling effect on freedom of expression

Malaysia’s legal environment already imposes heavy restrictions on free expression through the newly strengthened Section 233 of the Communications and Multimedia Act, the Sedition Act and other penal provisions that are often applied in ways that curb dissent, limit online spaces. Of particular concern is the fact that the soon-to-be-enforced Online Safety Act grants excessive and largely unchecked powers to the authorities to decide what content is considered “harmful”, risking the increased removal of lawful content. In this context, mandatory e-KYC would further expose users to identification and tracking, making us more vulnerable to state surveillance, selective enforcement, and self-censorship.

The introduction of e-KYC processes risks further eroding free expression in Malaysia by curbing online anonymity. Anonymity is essential for protecting the privacy and security necessary for exercising freedom of opinion and expression.

Social media has been a tool for advocacy and discourse, including through anonymous or pseudonymous speech, allowing human rights defenders, activists, journalists, whistleblowers, victims of abuse of power, and dissenting voices to have the space to speak without fear of reprisal or censorship. This is especially so for communities at risk, whose vulnerability or marginalisation may expose them to disproportionate targeting, thus having legitimate reasons to guard their identity.

When online anonymity is stripped away, individuals are far more likely to be investigated or prosecuted for expressing critical views or dissent. Users may then self-censor, and avoid posting legitimate criticism, comments or exposure of corruption or wrongdoing out of the fear of reprisal or persecution. Increased online regulation also risks resulting in social media companies taking a precautionary approach, which could lead to pre-publication censorship and the takedown of legitimate expressions. Mandatory identity verification under such restrictive and less transparent conditions would therefore have a massive chilling effect, and limit democratic spaces.

Beyond the risk to expression, mandatory e-KYC would disproportionately exclude persons or communities at risk, including undocumented persons, refugees, the LGBTQIA+ community, elderly people, and those living in rural or remote areas with limited connectivity. Limiting access to social media platforms undermines their ability to participate in public access to essential information and connect with support networks. In practice, such a policy could widen existing inequalities and reinforce systemic barriers that already leave vulnerable communities behind.

3. More crimes and harms for all users

Current e-KYC solutions are still subject to risks of fraud, data leaks, data loss, human, and technical errors. With every technological advancement, criminals will continue to seek to adapt and exploit these systems. At the same time, [a user uploading their biometric data and government-issued documents on the platform cannot be certain](#)

that it will never be further shared or even sold, and so create a potentially lasting digital footprint, make them vulnerable to the crimes the e-KYC policy is aiming to curb.

Additionally, there has been no transparency regarding mitigation and communication plans in cases of system failures, nor have there been any reports on the rigorous testing of the system intended for use. In Australia, the [Age Assurance Technology Trial](#) showed that there is no single solution that fits all contexts. With the government's haste, the policy will not be effective as intended, and instead lead to more unnecessary risks and costs to users who may be accidentally locked out of their social media accounts.

Recommendations

It is evident, based on the aforementioned risks and concerns, that introducing e-KYC within Malaysia's current socio-political climate will be more detrimental to human rights and the public interest than effective in addressing the harms as claimed by the government. We deplore that the measure was proposed without any prior consultation or engagement with relevant stakeholders, including civil society and affected communities. This absence of consultation undermines the legitimacy of the policy process and risks producing policies and regulations that are ineffective in curbing the real harm. Once more, we extend our invitation to the government for increased cooperation around digital regulations and policies. Civil society is more than willing to provide our expert insights and recommendations to strengthen online safety and regulations that serve the public interest. We believe that fostering a culture of participation and transparency is essential to building policies that are effective, rights-based, and trusted by the public.

We urge the government to **halt this hasty measure** and implement a multistakeholder, multidisciplinary approach that takes into account the interests of all groups within Malaysia, building a lasting system that can combat online harms while protecting the peoples' human rights. We further urge the government to:

- Embark on a **public consultation process**, with various groups from a range of socioeconomic levels, cultures, geographical regions and backgrounds to tackle the root causes of online harm while maintaining their autonomy and interests.
- Establish a **social media council** which would promote an independent multi-stakeholder regulatory framework to combat online harms. This body could also **review the root causes**, and the systemic and design-based failures of the social media platforms, and relatedly, develop a comprehensive plan of action.
- Conduct and make public **risk and human rights impact assessments** before introducing any new laws, policies or regulations that would have a significant impact on the right to privacy, data protection and the protection of all other human rights.
- Uphold the **right to information, open governance and promote transparency**. This would also include the promotion of algorithmic transparency and safeguards against discriminatory profiling as part of content moderation, targeting, or surveillance, and ensure they do not reproduce or exacerbate bias.
- Undertake a **complete review and reform of inadequate or repressive laws which undermine freedom of expression, data protection and privacy in Malaysia**, including placing an immediate moratorium on the use, pending amendments or repeal, of repressive laws including the Printing Presses and Publications Act (PPPA) 1984, the Official Secrets Act (OSA) 1972, the

Sedition Act 1948 and Section 233 of the Communications and Multimedia Act (CMA) 1998.

- **Amend the PDPA** to expand its scope of application to include government agencies and strengthen enforcement powers to ensure both public and private actors uphold the same obligations and are held accountable. In the same vein, the government must **amend the Data Sharing Act** to prevent indiscriminate inter-agency data sharing, and ensure transparency and accountability regarding how data is accessed, exchanged or used.
- Enhance its **education and awareness programmes** aimed at building a resilient society guided by ethical and responsible content creation standards, and with adequate digital literacy to combat the dangers of harmful content.

In conclusion, the government must go beyond political and economic expedients and reconsider its current plan. We must address the root and systemic causes of online harms before adopting any measures that could undermine human rights rather than significantly protecting the Malaysian public within the digital ecosystem.

Engaging with civil society organisations and the public at large can provide insights into the broader societal and systemic problems that contribute to harmful content and help develop more comprehensive and effective strategies for mitigating these harms.

4 October 2025

For further inquiries, please contact Lim Jih-Ming at comms@cijmalaysia.net