The Social and Civil Rights Implications of Mandatory Mobile National Digital Identity: An Analysis of Malaysia’s MyDigital ID Ecosystem

Disclosure and Disclaimer:
AI tools were used to discover sources, extract summaries, and compile drafts for this report. While the final report has been vetted and edited by human reviewers and editors, mistakes or omissions may happen. Sources/citations are indicated and listed for your reference and examination. This work has not undergone formal peer review and does not represent the official position of any authority or institution.
—

The global acceleration toward digitized public infrastructure has positioned national digital identity systems as the cornerstone of modern statecraft. Promoted as instruments of bureaucratic efficiency, fraud reduction, and seamless citizen-state interaction, these systems are increasingly deployed via mobile applications. However, the transition from physical identification to mandatory mobile digital identification represents a profound architectural shift in the relationship between the sovereign state and the citizen. When implemented without robust, decentralized privacy safeguards and strict legal limitations, mandatory mobile digital IDs introduce systemic vulnerabilities that threaten civil liberties, social inclusion, and democratic resilience.

This comprehensive analysis examines the social and civil rights risks inherent in mandatory mobile national digital IDs, utilizing Malaysia’s MyDigital ID program as a primary case study. Set against the backdrop of Malaysia's aggressive digitalization timeline leading into 2026, the report evaluates the intersection of state surveillance capabilities, historical technological governance failures, asymmetrical data protection frameworks, and the corporatization of sovereign identity.

The Architecture of Informational Control: Technical Mechanisms of Risk

The fundamental danger of a mobile-based national digital identity lies not merely in its digitized format, but in its underlying network architecture. Physical identification cards operate on a decentralized, peer-to-peer verification model. When an individual presents a physical card to a verifier, such as a pharmacist, a building security guard, or a bartender, the interaction remains strictly localized. The issuing authority is completely unaware that the verification event occurred. Mobile digital IDs, particularly those reliant on centralized authentication servers, fundamentally disrupt this localized privacy model by introducing persistent telemetry and server-side validation.

The "Phone Home" Phenomenon and Real-Time Behavioral Tracking

The most pervasive surveillance threat embedded in mobile digital ID systems is the capability to "phone home".[1] In systems where cryptographic validation requires a live application programming interface (API) connection to a government server, the state issuer receives a real-time data ping detailing exactly when and where the digital ID is being utilized.[1]

Through intentional state surveillance, secondary collusion with private sector entities, or merely as a byproduct of default configuration choices, the government can accumulate a comprehensive metadata log of a citizen's daily life.[1] This architecture effectively transforms an identification tool into a ubiquitous tracking mechanism. If a digital ID is mandated for a wide array of public and private services, the state gains the capacity to learn every time a citizen enters a specific commercial premises, purchases restricted medication, logs into a digital service, or accesses sensitive online content.[1]

The consolidation of informational power through routine verification logs replicates and intensifies existing sociopolitical power imbalances.[3] In contexts of rising political polarization or authoritarianism, the aggregation of metadata (timestamps, IP addresses, geolocation data, device identifiers, and relying party service names) facilitates predictive profiling.[3] By mapping an individual's behavioral patterns, the state can infer political affiliations, religious practices, and social networks with extreme granularity. As noted by civil society observers, this scenario is chilling in the context of global democratic backsliding, creating an environment where every interaction requires a digital permission slip from the state.[1]

The Fallacy of "Zero Data Storage" and Metadata Supremacy

Proponents of centralized digital IDs, including the developers of Malaysia's MyDigital ID, frequently argue that these platforms are secure because they do not "store" personal biometric data locally on the device or in new centralized repositories, but merely act as a

conduit to verify identity against existing national registries like the National Registration Department (JPN).[5] This defense, however, conflates database duplication with transactional surveillance. While the digital ID application may not retain a localized copy of a citizen's fingerprint or facial map, the authentication gateway processes and records the transactional metadata of every verification event.[6]

In digital forensics, intelligence gathering, and state surveillance, metadata is routinely more valuable than the core substantive data itself. Knowing that a specific citizen's identity was verified by an application belonging to an opposition political party, an investigative journalism outlet, or a reproductive healthcare clinic provides the state with highly actionable intelligence, regardless of whether the citizen's actual biometric template is held in a separate, secure silo.[3]
The failure to implement zero-knowledge proofs (ZKPs), cryptographic methods allowing a user to prove they possess a valid credential without revealing the credential itself or notifying the issuer, leaves the architecture fundamentally hostile to privacy.[9]

The MyKad Precedent vs. Centralized Authentication

The shift from physical to mobile ID represents a significant architectural pivot regarding transactional privacy. Malaysia's existing physical identification card, MyKad, introduced in 2001, operates as a multi-purpose smart card equipped with a secure chip platform and symmetric-key cryptography[53]. Crucially, MyKad supports localized, offline identity verification. When a citizen presents their MyKad to an authorized reader, the cryptographic verification occurs locally between the card's chip and the device's Secure Access Module (SAM)[54]. Because this process does not inherently require a real-time connection to a centralized database to prove identity, the state does not receive a persistent telemetry log of every individual transaction.

While the government maintains that MyDigital ID is meant to "complement rather than replace" MyKad for physical transactions, the mandatory integration of MyDigital ID for digital state services—such as MyJPJ and the MyNIISe immigration system—effectively shifts citizens into a centralized authentication model.

Experts have noted that MyKad's existing physical infrastructure could be upgraded to support true decentralization. Academic proposals suggest evolving national IDs into digital identity wallets utilizing blockchain and Self-Sovereign Identity (SSI) principles[55].

This decentralized approach would allow citizens to use Zero-Knowledge Proofs (ZKP), for instance, allowing a hospital to verify age or health eligibility via a smart contract without exposing the user's full identity or the state's central database. By prioritizing a centralized Single Sign-On (SSO) application over decentralized, hardware-backed verifiable

credentials, the current MyDigital ID trajectory risks abandoning the privacy-preserving potential of the physical IC card in favor of centralized telemetry and a potential single point of failure[56].

Alternative Paradigms: Decentralization and Data Minimization

The risks of "phoning home" and centralized telemetry are not inevitable technological mandates; they are deliberate architectural choices. Alternative models prioritize decentralized verification and privacy by design. For example, the State-Endorsed Digital Identity (SEDI) framework pioneered in Utah emphasizes a decentralized approach where citizens share only the minimum necessary cryptographic data, and the system is legally and technically barred from tracking usage by third parties.[9] SEDI explicitly outlaws third-party tracking and forces a strict data minimization protocol where citizens can selectively disclose attributes (e.g., proving they are over eighteen without revealing their exact date of birth or home address).[9]

Architectural Feature	Centralized Mobile ID (Default Model)	Decentralized Mobile ID / IC Smart Card	Civil Rights and Social Implications
Authentication Logic	Verification requires a server ping back to the issuer (Phones Home).	Cryptographic verification happens locally or via decentralized peer-to-peer protocols.	Centralized models allow real-time behavioral tracking; decentralized models preserve offline privacy and anonymity.
Data Disclosure	Often shares a full identity profile or creates centralized access logs.	Enables selective disclosure (e.g., proving age without revealing identity).	Selective disclosure protects users from commercial data scraping and targeted state profiling.
Revocability and Control	State can instantly revoke the ID, immediately locking the citizen out of all integrated services.	Revocation requires updating distributed registries; temporary offline use may still be possible.	Centralized instant revocation provides states with a "kill switch" over an individual's civic and economic participation.
Third-Party Doctrine	Data is continuously routed through third-party relays, compromising legal privacy protections.	Data remains under the cryptographic control of the end-user.	Decentralization closes surveillance loopholes that allow law enforcement to access data without warrants.

The Malaysian Digital Trajectory: MyDigital ID and the Coercion of Adoption

Malaysia's MyDigital ID serves as a critical, real-time case study in the rapid deployment of state-backed digital identity infrastructure. Developed under the auspices of MIMOS Berhad - a strategic agency under the Prime Minister's Department - and operated by its subsidiary MyDigital ID Sdn Bhd, the system is designed to serve as a unified Single Sign-On (SSO) authentication gateway for both public and private sector services across the nation.[5]

The government's trajectory reveals an aggressive timeline, transitioning the system from a voluntary convenience to a mandatory requirement. While initially positioned as an optional service for tech-savvy early adopters, regulatory shifts leading into 2026 demonstrate a concerted effort by the state to coerce adoption by tying the digital ID to essential state services, effectively holding civic participation hostage to technological compliance.

Manufactured Consent and the Public Relations Apparatus

A national digital identity system requires mass adoption to function as an effective digital public infrastructure.[13] Faced with initial public apathy and deep-seated skepticism regarding data privacy, evidenced by only 1.8 million early adopters out of a target population of millions by early 2024, the Malaysian government recognized a severe trust deficit.[7] The public's hesitation was rational, driven by Malaysia's status as a regional hotspot for scams, fraud, and historical government data breaches.[13]

In response, the state did not structurally alter the technology to be more privacy-preserving; instead, it engaged "Mechanikos," a public relations and marketing agency, to execute a comprehensive perception management campaign.[13] Recognizing that nearly half of the public harbored severe concerns about data privacy, the campaign deployed influencer-led explainers focusing heavily on MyDigital ID's "Common Criteria EAL3+" security standard.[13] By translating technical security jargon into emotive, culturally resonant content across Malaysia's diverse linguistic landscape, the campaign aimed to substitute genuine architectural privacy with a feeling of security.[13]

This strategy yielded numerical results. By early 2026, registrations surged to 8.7 million users, with the government targeting 15 to 17 million users by the end of the year.[13] The system integrated with over 80 government and private-sector applications, processing over 400,000 weekly logins.[13] However, high adoption rates driven by marketing and influencers do not equate to informed consent regarding the long-term civil liberties implications of the infrastructure.

The Transition to Mandatory Integration

The true mechanism of adoption for MyDigital ID has not been public relations, but

regulatory coercion. The state aims to integrate 95 percent of all public services with the digital ID by 2030, transforming the platform from an option into a daily necessity.[13]

By early 2026, the state announced that MyDigital ID would become the sole login method for critical applications. The Road Transport Department (JPJ) scheduled the mandatory integration of MyDigital ID for the MyJPJ app—a necessity for citizens to manage digital driving licenses and road tax.[17] Originally scheduled for February 2026, administrative and technical delays forced postponements to May 1, 2026.[17]

Similarly, the Home Ministry mandated MyDigital ID as the exclusive sign-on platform for the National Integrated Immigration System (MyNIISe) mobile app, effective January 15, 2026, making it a prerequisite for Malaysian citizens traveling abroad and interacting with border control at major terminals like KLIA 1 and KLIA 2.[5] While foreign travelers are currently exempt, Malaysian citizens aged 18 and above are effectively forced into the ecosystem to exercise their right to freedom of movement.[16]

This transition fundamentally alters the social contract. When a mobile digital ID becomes a prerequisite for crossing a border, renewing a vehicle tax, or accessing federal systems, the state holds an administrative chokehold over the individual. It ceases to be an identity system and becomes a continuous licensing system for basic human activity.

Historical Precedents and the Deficit of Public Trust

Public resistance to mandatory digital IDs in Malaysia is not born of technological Luddism; it is a highly rational response to a documented, recent history of state failures in managing digital infrastructure. The drive toward MyDigital ID is haunted by the catastrophic security failures, governance scandals, and data leaks of previous state applications.

The MySejahtera Data Breach and the Illusion of State Ownership

During the COVID-19 pandemic, the Malaysian government mandated the use of the MySejahtera mobile app for contact tracing and vaccination records. Despite repeated, forceful assurances from the Health Ministry that citizen data was highly secure and owned entirely by the Malaysian government, the system suffered massive structural failures.[20]

The Auditor-General's 2021 report revealed a devastating breach: a single "Super Admin" account within the MyVAS system was utilized to illicitly download the highly sensitive personal and medical data of three million vaccine recipients.[22] The breach, executed between October 28 and October 31, 2021, across five different IP addresses, highlighted a catastrophic lack of internal auditing, access control, and compartmentalization.[22] The incident necessitated interventions by the National Cyber Security Agency (NACSA) and police investigations.[22]

Furthermore, the Malaysian Bar and Parliament's Public Accounts Commission raised severe alarms regarding the opacity of the app's corporate structure. It was discovered that the software was legally owned by a foreign entity—a Singaporean company named Entomo Pte Ltd (previously KPISoft Malaysia Sdn Bhd)—appointed through a direct, non-tendered cabinet decision.[20] The MySejahtera debacle established a grim precedent for the Malaysian public: state assurances of absolute data security are functionally meaningless when confronted with insider threats, unaccountable private vendors, offshore corporate ownership, and inadequate technical architecture.

PADU and the Resistance of the Periphery

The launch of the Pangkalan Data Utama (PADU), or Central Database Hub, further eroded public trust in state data consolidation. Designed to centralize vast arrays of socioeconomic data for targeted subsidies, PADU was immediately met with widespread skepticism regarding data sovereignty and institutional vulnerability.[23] This distrust was heavily amplified by Malaysia's unenviable status as the eighth most breached country globally in the third quarter of 2023, with nearly half a million accounts compromised.[23]

Crucially, the PADU initiative triggered a constitutional and political crisis regarding data federalism. The state government of Sarawak halted its participation in PADU in March 2024, citing explicit fears over data sovereignty and the storage of citizens' personal data outside the state's jurisdiction.[23] Sarawakian ministers openly expressed fears that the centralized data could be weaponized for political microtargeting or state surveillance during elections.[23] Sarawak's rebellion underscores a fundamental geopolitical reality within federal systems: centralized digital databases are viewed by regional actors and opposition parties not merely as administrative tools, but as weapons of informational dominance that threaten the balance of political power.

MIMOS and the MyDigital ID Governance Scandal

The legitimacy of MyDigital ID has been severely compromised before reaching full adoption by the devastating findings of the Auditor-General's Report (LKAN) 1/2026.[24] MIMOS Berhad, the state agency entrusted with the development and implementation of MyDigital ID, was found to have circumvented core governance protocols, resulting in RM28.13 million in unauthorized or unapproved expenditures.[24]

The audit revealed a staggering breakdown in internal controls. MIMOS utilized RM14.09 million of development funds to cover routine operating expenses, including staff emoluments, resource costs, and office equipment.[24] This direct violation of the 12th Malaysia Plan (12MP) Development Project Implementation Guidelines indicated that expenditures did not comply with the approved purpose of the vote.[24] Across 11 project sub-scopes, funds were spent in excess of allocations or without any allocation whatsoever.[24]

The governance structure of the project completely collapsed. The audit highlighted that there were no formal presentations regarding expenditure approvals or project implementation status during monitoring meetings.[24] The board of directors' representative from MIMOS was cited for failing to exercise fundamental fiduciary responsibilities, and the agency failed to comply with conditions imposed by the Home Ministry.[24] Furthermore, procurement processes were bypassed entirely for the purchase of security cages and door access systems, which were subsequently never utilized, resulting in pure financial wastage and exposing deep weaknesses in asset control.[24]

This financial and administrative scandal is intrinsically linked to civil rights and cybersecurity risks. If the agency responsible for constructing the nation's cryptographic identity gateway is incapable of managing basic financial controls, adhering to procurement guidelines, or preventing the wastage of millions, it fundamentally lacks the institutional competence to safeguard the biometric and transactional data of over 20 million citizens.[24] Governance failures in software development translate directly into zero-day vulnerabilities, API leaks, and vulnerability to advanced persistent threats (APTs).

Historical Digital Initiative	Year of Major Controversy	Core Failure / Vulnerability	Civil Rights / Privacy Implication
MySejahtera	2021-2022	"Super Admin" breach of 3M records; Opacity in private vendor ownership (Entomo Pte Ltd).[20]	Medical privacy violated; demonstrated the state's inability to secure sensitive personal health data against insider threats.
PADU	2024	Centralization of socioeconomic data; Outdated security methods; State resistance.[23]	Fears of political microtargeting and state surveillance; sparked inter-state data sovereignty disputes (Sarawak).[23]
MyDigital ID	2026	RM28.13M unapproved spending by MIMOS; Misuse of development funds; Fiduciary failure.[24]	Institutional incompetence indicates severe risk to biometric data integrity and future system architecture security.

The Illusion of Legal Safeguards: Regulatory Voids and State Exemptions

A common defense of mandatory digital ID systems is that potential technical risks will be mitigated by robust legislative frameworks. However, an analysis of Malaysia's legal landscape heading into 2026 reveals a deeply asymmetrical regulatory environment designed to bind the private sector while granting the state near-total impunity regarding citizen data.

The PDPA 2024 Amendments: A Shield with a Massive Loophole

The Personal Data Protection (Amendment) Act 2024 (enforced in three phases: January, April, and June 2025) represents the most significant modernization of Malaysia's privacy laws since 2010.[26] The amendments were designed to align Malaysia closer to international standards, introducing mandatory data breach notifications to the Commissioner and data subjects, enforcing direct legal obligations on data processors to maintain security principles, mandating the appointment of Data Protection Officers (DPOs), and introducing the right to data portability.[27] Furthermore, biometric data has been explicitly categorized as "sensitive personal data," requiring a higher threshold of care.[27] The financial penalties for non-compliance were drastically increased to a maximum of MYR 1 million and up to three years imprisonment.[27]

While these reforms force corporate entities into stringent compliance, they contain a fatal, structural flaw regarding state surveillance: **The PDPA explicitly does not apply to the Federal Government or State Governments.** Section 3 of the principal Act, which comprehensively exempts government agencies from the PDPA, was neither repealed nor altered by the 2024 amendments.[31]

This profound legal asymmetry dictates that while a private corporation can be fined millions and its directors jailed for exposing a citizen's data, the government departments managing MyDigital ID, MyNIISe, and MyJPJ operate entirely outside the jurisdiction of the national privacy law.[31] If the National Registration Department (JPN), the Home Ministry, or MIMOS suffers a catastrophic breach of digital ID transactional metadata, they are under no statutory obligation to notify the public, nor are they subject to the punitive measures outlined in the amended PDPA. For the citizen, this means that their mandatory digital identity is aggregated, processed, and managed by an entity possessing total legal immunity from the nation's premier data protection framework.

The Public Sector Data Sharing Act 2025: Expanding the State Dragnet

Rather than subjecting itself to the rigors of the PDPA, the Malaysian government introduced the Data Sharing Act 2025 (in force as of April 28, 2025).[34] While pitched publicly as a framework to ensure "secure and efficient" sharing of data between public sector

agencies, the Act functions effectively as a legal mechanism to consolidate the state's informational power and legalize a massive data dragnet.[34]

The Act defines "data" far more broadly than the PDPA's definition of "personal data." Under the Data Sharing Act, data encompasses "any facts, statistics, instructions, concepts or other information in a form that is capable of being communicated, analysed or processed".[34] It empowers agencies like the police force, armed forces, educational services, and the general public service to routinely request and share citizen data through the newly established National Data Sharing Committee and the National Digital Department.[34]

When contextualized alongside the mandatory rollout of MyDigital ID, the Data Sharing Act is deeply concerning. The digital ID serves as the unified index key for a citizen across all disparate government platforms. The Data Sharing Act provides the legal lubricant for these formerly siloed databases to be merged and cross-referenced with frictionless efficiency. A citizen's digital ID login at a government hospital can legally be shared with the police force or the inland revenue authority under the guise of "national security," "investigation of a breach," or broad public interest.[34]

While the Act contains severe penalties for individual officers or servants of public agencies who use or disclose shared data for unauthorized purposes (up to RM1 million in fines or five years imprisonment) [34], it fundamentally lacks the mechanisms of individual consent, transparency, and the right to object that are foundational to human rights-based data regimes. Citizens are not granted rights to access or correct the data the state aggregates on them under this Act, leaving them entirely blind to how their digital identity metadata is traded across ministries.[36]

The MCMC Metadata Directives and Sectoral Overreach

The state's appetite for granular surveillance is already evident beyond the scope of identity apps. In early 2025, the Malaysian Communications and Multimedia Commission (MCMC) issued a highly controversial directive instructing Mobile Network Operators (MNOs) to disclose massive volumes of mobile phone metadata to the government for the "Mobile Phone Data" (MPD) program.[8] The directive, backed by threats of criminal penalties under the Communications and Multimedia Act (CMA), demanded mobile call records for "official statistical purposes".[37]

The Malaysian Bar strongly condemned this action, noting the severe public unease regarding the state aggregation of real-time data, even if purportedly anonymized for infrastructure planning.[37] If the state is willing to coerce MNOs into surrendering cellular metadata en masse, it requires very little extrapolation to foresee the vast transactional logs generated by MyDigital ID being co-opted for similar mass surveillance purposes under the auspices of the Data Sharing Act.

Civil Liberties, Free Expression, and the Digital Panopticon

The deployment of a mandatory national digital ID does not occur in a regulatory vacuum; it interacts synergistically with other legislative frameworks to consolidate state control. In Malaysia, the intersection of MyDigital ID with impending draconian internet regulations presents an existential threat to freedom of expression, political dissent, and journalistic integrity.

The Online Safety Act (ONSA) and the End of Anonymity

The Malaysian government's intent to enforce the Online Safety Act (ONSA) by late 2025 or early 2026 introduces a severe requirement for all social media and messaging platforms operating in the country to implement mandatory electronic Know-Your-Customer (e-KYC) verification.[38] Announced by the Minister of Communications, Fahmi Fadzil, this directive mandates that users verify their social media accounts using government-issued documents, explicitly naming MyDigital ID as the primary verification tool.[38]

This policy effectively obliterates online anonymity. Anonymity is not merely a shield for criminality, as state security apparatuses often claim; it is a fundamental prerequisite for democratic discourse, allowing human rights defenders, whistleblowers, journalists, and victims of abuse to express themselves without fear of state or corporate reprisal.[38] By inextricably linking a citizen's state-verified digital identity to their online avatars, the government gains the unprecedented ability to monitor digital behavior, map political associations, and infer emotional or ideological states based on metadata.[38]

Civil society groups, including the Centre for Independent Journalism (CIJ), ARTICLE 19, and Sinar Project, have explicitly warned that this fusion of identity and expression carries a profound chilling effect.[38] When citizens know that their comments on news articles, their participation in political forums, and their social media activism are directly tethered to their national identity number, self-censorship becomes an automatic survival mechanism.[38] This dynamic is dangerously exacerbated by Malaysia's history of utilizing sweeping legislation, such as the Sedition Act 1948, the Security Offences (Special Measures) Act 2012 (SOSMA), and Section 233 of the CMA, to suppress legitimate dissent and target political opponents.[38]

Algorithmic Profiling and Pre-Publication Censorship

The integration of national digital IDs with social media e-KYC protocols facilitates algorithmic profiling on a mass scale.[38] When state authorities, such as the MCMC, are granted unchecked powers under ONSA to define "harmful" content, social media companies, facing immense legal liability and new licensing requirements effective August 2024, are incentivized to adopt a "precautionary approach".[38]

This results in the automated suppression of content and widespread pre-publication censorship. Furthermore, algorithmic risk scores attached to verified digital IDs can be utilized to shadow-ban activists or throttle the reach of opposition narratives. The digital ID transitions from a tool of authentication into a mechanism of behavioral control, where access to the digital public square is contingent upon state-defined compliance.[4] This phenomenon has been termed the "Internet Lockdown" - a bureaucratic wall erected between citizens and their constitutional rights to seek and share information.[4]

Threats to Legal Professional Privilege and Civic Assembly

The digitalization of identity and communication also threatens foundational legal doctrines, most notably legal professional privilege and confidentiality (LPPC). Organizations such as Lawyers for Liberty, SUARAM, and the Malaysian Bar have repeatedly warned against the state's encroachment on digital communications and civil rights.[39] If a mandatory digital ID becomes embedded in legal communication networks, electronic court filing systems, or secure messaging protocols used by attorneys, the metadata generated by these interactions becomes highly vulnerable to state interception.[42]

The tracking of digital footprints allows state prosecutors or intelligence agencies to map networks of association between defense attorneys, their clients, and potential whistleblowers. The loss of secure, unmonitored channels of communication undermines the right to a fair trial and cripples the ability of civil society to mount legal challenges against state overreach.[42] Furthermore, human rights groups like SUARAM have documented the state's persistent efforts to undermine physical assemblies using the Protected Places and Protected Areas Act (PAPPA) and the Peaceful Assembly Act (PAA).[39] Coupling a state hostile to physical protest with a digital infrastructure capable of tracking individuals via their mobile IDs creates a seamless web of suppression, deterring citizens from participating in democratic life both online and offline.

Social Inclusion, Accessibility, and the Digital Divide

The imposition of a mandatory mobile digital ID generates severe externalities for social equity. A digital-first, mobile-centric approach inherently privileges the technologically literate, the financially secure, and the geographically connected, while systematically disenfranchising vulnerable demographics.[38]

The Disenfranchisement of Marginalized Communities

Civil society organizations warn that mandatory electronic verification will disproportionately impact marginalized communities.[38] A mobile-app-based digital ID assumes that the user possesses a modern smartphone capable of running current operating systems, a stable internet connection, and the digital literacy required to navigate

complex biometric onboarding processes, which include multi-angle facial scanning, eKYC document captures, and One-Time Passwords (OTPs).[45]

For rural populations in states like Sabah and Sarawak, where telecommunications infrastructure remains highly uneven and broadband penetration is lacking, this requirement poses an insurmountable barrier to entry.[46] Similarly, the elderly, individuals in lower socio-economic strata, undocumented persons, and refugee communities are frequently excluded from digital ecosystems.[38] If access to essential government services—including healthcare, welfare distribution, and immigration—is gatekept behind a digital ID, these vulnerable groups face total exclusion from the social safety net, exacerbating existing poverty and inequality.[3]

The Inadequacy of Physical Kiosks and Biometric Discrimination

In an attempt to mitigate these accessibility concerns, MyDigital ID implementers have deployed physical kiosks and explored alternative biometric verification methods for individuals who lack smartphones or suffer from degraded fingerprints due to manual labor.[7] However, relying on physical kiosks as a primary fallback mechanism introduces its own set of systemic failures.

Physical kiosks are geographically bound and often clustered in urban centers, commercial nodes, or specific franchise locations (e.g., Tealive kiosks in Penang or Selangor), maintaining the barrier of physical access for rural populations.[46] Furthermore, a citizen who registers via a kiosk but does not possess a personal smartphone cannot utilize the mobile-centric features of the digital ID for daily transactions or sudden administrative needs.[6] This creates a bifurcated society: first-class citizens who navigate the digital state seamlessly via personal devices, and second-class citizens tethered to state-operated terminals, subject to public scrutiny, long queues, and restricted autonomy. Moreover, biometric systems frequently exhibit higher failure rates for individuals with darker skin tones, facial anomalies, or skin conditions, introducing algorithmic discrimination into the very foundation of civic identity.[7]

The Private Sector Nexus: Monetization and Monopolistic Integration

The risks of state surveillance and exclusion are exponentially compounded by the deep integration of private commercial entities into the MyDigital ID ecosystem. The platform has actively pursued partnerships with the private sector, seeking to embed the sovereign identity layer into commercial applications.

Special Note
While various sources cite MYEG's collaboration with MyDigital ID Solutions Sdn Bhd (MYIDSSB), no official information or business registration was found for the latter. Citation reference #47 reports that MYIDSSB is a wholly-owned subsidiary of MIMOS, and this is also mentioned in a statutory securities announcement by MYEG's subsidiary (https://myeg.irplc.com/new-announcement.htm?NewsID=202508135000008&Symbol=0138).

MYEG and the Corporatization of Sovereign Identity

A notable development in this space is the collaboration between MyDigital ID Solutions Sdn Bhd and MY E.G. Services Berhad (MYEG), a dominant digital services provider in Malaysia.[47] Together, they have launched the "MyDigital ID Superapp," built on Malaysia's Blockchain Infrastructure, which integrates blockchain and digital identity technologies with commercial e-wallets, news broadcasting features, and mini-apps.[47]

This public-private fusion creates a highly porous boundary between state identity registries and commercial data brokers. Integrating the national ID directly into private superapps expands the attack surface for data breaches and creates immense commercial incentives to aggregate user data. When citizens are forced to utilize a privately operated superapp to access their sovereign identity, their transactional data becomes collateral for corporate monetization, fundamentally eroding the principles of data minimization.[47]

The Risk of Monopolistic Abuse

The choice of MYEG as a premier partner raises significant anti-competition and civil rights concerns. MYEG has a documented history of monopolistic practices within Malaysia's digital economy. The Malaysian Competition Commission (MyCC) previously fined MYEG MYR 9.64 million for abusing its dominant position by forcing employers to purchase Foreign Workers Insurance Guarantees through its platform, creating deliberate delays for those who opted for competing insurers.[50]

Entrusting the facilitation of a national digital identity to a corporation with a penalized history of anti-competitive coercion is highly problematic. It raises the distinct possibility

that the digital ID ecosystem could be manipulated to lock citizens into specific commercial ecosystems, forcing them to adopt proprietary e-wallets or insurance products as a prerequisite for seamless government interaction.[48] This transforms a public utility into a monopolistic tollbooth, where civil rights are commodified.

Strategic Recommendations and Conclusion

The empirical record and structural analysis demonstrate that the current trajectory of mandatory mobile digital IDs—specifically the Malaysian model progressing into 2026—poses unacceptable risks to civil rights, privacy, and democratic stability. The combination of centralized telemetry, coercive adoption mandates, catastrophic historical governance failures, asymmetrical legal protections, and corporate entanglement creates an infrastructure primed for abuse.

To mitigate these severe threats and transition toward a rights-respecting framework, systemic architectural, legal, and operational reforms are imperative:

1. **Enforce Cryptographic Decentralization and Eradicate Telemetry:** Governments must abandon centralized authentication servers that inherently "phone home".[1] Digital ID systems must be rebuilt upon decentralized architectures—similar to the Utah SEDI model—utilizing Zero-Knowledge Proofs (ZKPs) and Verifiable Credentials (VCs).[9] This ensures that verification occurs locally or peer-to-peer between the citizen and the relying party, leaving absolutely no metadata trail for the state or corporate entities to harvest.
2. **Guarantee Absolute Voluntariness and Preserve Analog Alternatives:** Digital identity must legally remain a strictly voluntary service.[44] The state must mandate the preservation of physical, analog alternatives for all critical government services without penalty or artificial delay. Coercive mandates, such as tying digital IDs to driver's licenses (MyJPJ) or immigration portals (MyNIISe) by set deadlines, must be permanently reversed to protect marginalized communities, rural populations, and the technologically disenfranchised.
3. **Abolish State Exemptions in Privacy Legislation:** The fundamental legal asymmetry protecting the state must end. Section 3 of the Malaysian PDPA must be repealed, fully subjecting federal and state government bodies to the exact same rigorous data protection standards, mandatory public breach notifications, and punitive financial and criminal liabilities applicable to the private sector.[32] A digital ID cannot be trusted if the agencies operating it (such as JPN, MIMOS, and the Home Ministry) exist entirely above the law.
4. **Halt Mandatory e-KYC for Public Discourse and Repeal ONSA:** Initiatives like the Online Safety Act (ONSA) that mandate identity verification for social media and communications platforms must be immediately abandoned.[38] The right to anonymous speech is central to civil liberty and the protection of whistleblowers and human rights defenders. The state must construct an impenetrable firewall separating

sovereign identification from digital expression.

5. **Establish Independent, Non-Executive Oversight:** Agencies responsible for digital infrastructure must be subjected to stringent, independent technical and financial audits, given the devastating RM28.13 million governance failure by MIMOS.[24] A permanent, independent parliamentary commission must be established to oversee the deployment, algorithmic functions, and data sharing activities of the digital identity ecosystem, equipped with the binding authority to suspend operations if civil rights are violated or financial irregularities are detected.
6. **Sever the Link Between Sovereign Identity and Corporate Monopolies:** The integration of the national digital ID into corporate superapps, particularly those operated by entities with histories of anti-competitive behavior, must be heavily regulated. The state must prevent the commercial collateralization of sovereign identity, ensuring that citizens are not forced to adopt private financial products or e-wallets to interact with their government.

The rush toward digitized governance must not be permitted to outpace the preservation of human rights. Without fundamental structural redesigns focusing on decentralization, legal accountability, and voluntary adoption, mandatory mobile national digital IDs will cease to function as tools of citizen empowerment. Instead, they risk evolving into turnkey totalitarian infrastructures, providing current and future administrations with the ultimate instruments of behavioral control and panoptic surveillance.

—

Works cited

1. Digital IDs Must Not Phone Home - Center for Democracy and Technology - CDT, accessed March 7, 2026, https://cdt.org/insights/digital-ids-must-not-phone-home/
2. ACLU Digital ID State Legislative Recommendations | American Civil Liberties Union, accessed March 7, 2026, https://www.aclu.org/publications/aclu-digital-id-state-legislative-recommendations
3. Digital IDs Put Health Care Privacy at Risk - Convergence Magazine, accessed March 7, 2026, https://convergencemag.com/articles/digital-ids-put-health-care-privacy-at-risk/
4. Digital Driver's Licenses Threaten to Create a “Great Internet Lockdown” - ACLU.org, accessed March 7, 2026, https://www.aclu.org/news/privacy-technology/the-internet-lockdown
5. What is MyDigital ID and MyNIISe — and why Malaysians now need both to travel, accessed March 7, 2026, https://www.malaymail.com/news/malaysia/2026/01/13/what-is-mydigital-id-and-myniise-and-why-malaysians-now-need-both-to-travel/204775
6. Get In Touch - MyDigital ID, accessed March 7, 2026, https://www.digital-id.my/en/support

7. MyDigital ID has secure and trusted layer for verification, says Deputy CEO - GovInsider, accessed March 7, 2026, https://govinsider.asia/intl-en/article/mydigital-id-has-secure-and-trusted-layer-for-verification-says-deputy-ceo
8. Malaysia's Metadata Controversy: Surveillance in the Guise of Statistics | FULCRUM, accessed March 7, 2026, https://fulcrum.sg/malaysias-metadata-controversy-surveillance-in-the-guise-of-statistics/
9. There's Only One State That is Asking the Right Questions About Digital Identity - ACLU.org, accessed March 7, 2026, https://www.aclu.org/news/privacy-technology/digital-id-utah
10. Digital Identity Leaders and Privacy Experts Sound the Alarm on Invasive ID Systems | American Civil Liberties Union - ACLU.org, accessed March 7, 2026, https://www.aclu.org/press-releases/digital-identity-leaders-and-privacy-experts-sound-the-alarm-on-invasive-id-systems
11. Closing the Third-Party Privacy Loophole - Libertas Institute, accessed March 7, 2026, https://libertas.institute/our-impact/closing-the-third-party-privacy-loophole/
12. Company Overview Vision Mission - MGTC, accessed March 7, 2026, https://www.mgtc.gov.my/wp-content/uploads/2024/07/MyDigital-ID-Sdn-Bhd-Vacancies-v6-30062024-1.pdf
13. MyDigital ID PR campaign targeting Malaysian diversity and misconceptions hailed a success | Biometric Update, accessed March 7, 2026, https://www.biometricupdate.com/202601/mydigital-id-pr-campaign-targeting-malaysian-diversity-and-misconceptions-hailed-a-success
14. Rewriting Malaysia's digital narrative: How MyDigital ID transformed public doubt into nationwide adoption - MARKETECH APAC, accessed March 7, 2026, https://marketech-apac.com/rewriting-malaysias-digital-narrative-how-mydigital-id-transformed-public-doubt-into-nationwide-adoption/
15. Malaysia targets 17 million MyDigital IDs by end-2026 - Biometric Update, accessed March 7, 2026, https://www.biometricupdate.com/202602/malaysia-targets-17-million-mydigital-ids-by-end-2026
16. Malaysia mandates MyDigital ID for Malaysians traveling abroad - Biometric Update, accessed March 7, 2026, https://www.biometricupdate.com/202601/malaysia-mandates-mydigital-id-for-malaysians-traveling-abroad
17. MyJPJ's MyDigital ID Implementation Postponed Yet Again; Now Set For 1 May 2026, accessed March 7, 2026, https://www.lowyat.net/2026/384704/myjpj-mydigital-id-postponed-to-1-may-2026/
18. MyDigital ID: Mandatory Login from 2026 — What It Means for Travel & How to Prepare, accessed March 7, 2026, https://www.klook.com/en-MY/blog/mydigitalid-login/
19. Confused About The MyDigital ID And MyNIISe Integration? Here's A Simple Explanation, accessed March 7, 2026, https://www.therakyatpost.com/news/2026/01/08/confused-about-the-mydigital-id-and-myniise-integration-heres-a-simple-explanation/

20. Press Release | Transparency and Protection of Privacy Crucial for ..., accessed March 7, 2026, https://www.malaysianbar.org.my/article/news/press-statements/press-statements/press-release-transparency-and-protection-of-privacy-crucial-for-personal-data-collected-through-the-mysejahtera-application
21. How MySejahtera's development became a data privacy concern: A timeline | Malay Mail, accessed March 7, 2026, https://www.malaymail.com/news/malaysia/2022/04/02/how-mysejahteras-development-became-a-data-privacy-concern-a-timeline/2051081
22. Audit: MySejahtera Data Breach Affected Three Million Users - CodeBlue, accessed March 7, 2026, https://codeblue.galencentre.org/2023/02/audit-mysejahtera-data-breach-affected-three-million-users/
23. Big Data, Bigger Debate: Malaysia's PADU System and the Future of ..., accessed March 7, 2026, https://fulcrum.sg/big-data-bigger-debate-malaysias-padu-system-and-the-future-of-digital-governance/
24. RM28.13 Mln MyDID Project Under MIMOS Spent ... - BERNAMA, accessed March 7, 2026, https://www.bernama.com/en/news.php?id=2526899
25. Auditor-General Flags RM28.13 Million In Unapproved MyDigital ID Project Spending, accessed March 7, 2026, https://www.lowyat.net/2026/383892/auditor-general-flags-rm28-13-million-in-unapproved-mydigital-id-project-spending/
26. Countdown to Compliance Personal Data Protection (Amendment) Act 2024 in Force Starting 1 January 2025 - Legal 500, accessed March 7, 2026, https://www.legal500.com/developments/thought-leadership/countdown-to-compliance-personal-data-protection-amendment-act-2024-in-force-starting-1-january-2025/
27. Part 1: Personal Data Protection (Amendment) Act 2024 - RÖDL, accessed March 7, 2026, https://www.roedl.com/en/insights/malaysia-personal-data-protection-amendment-act-2024/
28. From Legislative Reform to Practical Guidance: Key Amendments to Malaysia's PDPA and the Launch of Cross-Border Transfer Guidelines | Insights | Mayer Brown, accessed March 7, 2026, https://www.mayerbrown.com/en/insights/publications/2025/07/from-legislative-reform-to-practical-guidance-key-amendments-to-malaysias-pdpa-and-the-launch-of-cross-border-transfer-guidelines
29. Understanding Malaysia's 2024 Data Privacy Reform - Hall Booth Smith, accessed March 7, 2026, https://hallboothsmith.com/malaysia-2024-data-privacy-reform/
30. Malaysia: Personal Data Protection (Amendment) Bill 2024 - Baker McKenzie InsightPlus, accessed March 7, 2026, https://insightplus.bakermckenzie.com/bm/investigations-compliance-ethics/malaysia-personal-data-protection-amendment-bill-2024
31. Application and Non-Application of the Act • Personal Data Protection, accessed March 7, 2026, https://www.pdp.gov.my/ppdpv1/en/akta/application-and-non-application-of-t

he-act/
32. Malaysia: Personal Data Protection (Amendment) Act 2024 to come into force, accessed March 7, 2026, https://insightplus.bakermckenzie.com/bm/data-technology/malaysia-personal-data-protection-amendment-act-2024-to-come-into-force
33. PDPA amendments missing key details - ISIS, accessed March 7, 2026, https://www.isis.org.my/2024/07/30/pdpa-amendments-missing-key-details/
34. Malaysia enacts data sharing rules for public sector - Hogan Lovells, accessed March 7, 2026, https://www.hoganlovells.com/en/publications/malaysia-enacts-data-sharing-rules-for-public-sector
35. Data Sharing Act 2025 – Overview and Key Provisions., accessed March 7, 2026, https://www.rdslawpartners.com/post/data-sharing-act-2025-overview-and-key-provisions
36. Malaysia Parliament passes Data Sharing Bill 2024 : Allen & Gledhill, accessed March 7, 2026, https://www.allenandgledhill.com/publication/articles/29852/parliament-passes-data-sharing-bill-2024
37. Press Statement | Rebuilding the Public Trust Deficit With Regard to Personal Data Collection - The Malaysian Bar, accessed March 7, 2026, https://www.malaysianbar.org.my/article/news/press-statements/press-statements/press-statement-rebuilding-the-public-trust-deficit-with-regard-to-personal-data-collection
38. Malaysia: Halt hasty imposition of mandatory electronic verification - ARTICLE 19, accessed March 7, 2026, https://www.article19.org/resources/malaysia-halt-hasty-imposition-of-mandatory-electronic-verification/
39. Malaysia - Capacity4dev, accessed March 7, 2026, https://capacity4dev.europa.eu/media/282405/download/9c21b3e6-c15c-4ef0-bd3f-ced8d89325cb_en
40. Sosma review in the works - The Star, accessed March 7, 2026, https://www.thestar.com.my/news/nation/2025/02/15/sosma-review-in-the-works
41. Malaysia: Freedom on the Net 2024 Country Report, accessed March 7, 2026, https://freedomhouse.org/country/malaysia/freedom-net/2024
42. Lawyer-Client Confidentiality in a Digitalized Society, accessed March 7, 2026, https://www.lawyersforlawyers.org/report-lawyer-client-confidentiality-in-a-digitalized-society/
43. Malaysia: Freedom on the Net 2023 Country Report, accessed March 7, 2026, https://freedomhouse.org/country/malaysia/freedom-net/2023
44. Navigating the Risks and Rewards of Digital ID Systems | Open Government Partnership, accessed March 7, 2026, https://www.opengovpartnership.org/stories/navigating-the-risks-and-rewards-of-digital-id-systems/
45. Trusted Digital Identity for Secure Online Verification - MyDigital ID, accessed March 7, 2026, https://www.digital-id.my/en
46. MyDigital ID Kiosk Locations in Malaysia | PDF - Scribd, accessed March 7,

2026, https://www.scribd.com/document/819118436/Lokasi-Kios-MyDigital-ID
47. Malaysia's MyDigital ID Superapp: Revolutionizing Digital Identity and Security, accessed March 7, 2026, https://worldecomag.com/myeg-mydigital-id-blockchain-digital-identity/
48. Enabling Trusted, Inclusive Fast Payments through Digital ID - World Bank Documents & Reports, accessed March 7, 2026, https://documents1.worldbank.org/curated/en/099020526062040816/pdf/P512054-d38572c0-15e8-48e9-95f8-0e6de9e078b1.pdf
49. English Text (284.62 KB) - World Bank Open Knowledge Repository, accessed March 7, 2026, https://openknowledge.worldbank.org/bitstreams/0943845c-55c5-41ff-b39f-45e5122273d5/download
50. Market Review on the Digital Economy Ecosystem Under the Competition Act 2010, accessed March 7, 2026, https://www.mycc.gov.my/sites/default/files/2025-03/Public_Interim%20report%20for%20Market%20Review%20on%20the%20Digital%20Economy%20Ecosystem%20under%20the%20Competition%20Act%202010.pdf
51. Market Review on the Digital Economy Ecosystem Under the Competition Act 2010, accessed March 7, 2026, https://www.mycc.gov.my/sites/default/files/%5BBook%203%5D%20Draft%20final%20report%20(Digital%20advertising%20services).pdf
52. National Cybersecurity Chief: Malaysian national ID adoption must be voluntary, accessed March 7, 2026, https://www.biometricupdate.com/202507/national-cybersecurity-chief-malaysian-national-id-adoption-must-be-voluntary
53. **National Registration Department (JPN).** "MyKad - Superiority at Your Fingertips." jpn.gov.my.
54. **S.A.M. Aljunid, et al.** "On The Security Design Of MyKad." *ResearchGate*. View Publication.
55. **Naik, N.** (2021). "Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet." *Aston University*. Download PDF.
56. **IN Groupe.** "Advantages of Decentralized Digital Identity Architecture." ingroupe.com.