IRIS
Information Resilience & Integrity Symposium

RESEARCH PAPER

Good Governance and Development Nexus in Southeast Asian Digital Landscape

PANEL 2 | Surveillance and Privacy in Digital Development

Safer Internet Lab

Centre for Strategic and International Studies

Google

Universitas Gadjah Mada
Fakultas Ilmu Sosial dan Ilmu Politik

Center for Digital Society

Dr. Surachanee Sriyai

Dr. Surachanee "Hammerli" Sriyai is a Visiting Fellow of the Media, Technology and Society Programme at ISEAS – Yusof Ishak Institute, where she writes about digital politics in Southeast Asia, especially Thailand and Myanmar. She is also the interim director of the Center for Sustainable Humanitarian Action with Displaced Ethnic Communities (SHADE), a multi-stakeholder platform for cross-border collaboration between Thailand and Myanmar.

Good Governance and Development Nexus in Southeast Asian Digital Landscape

Dr. Surachanee Sriyai

This paper explores the intersection of digital development and governance in Southeast Asia, focusing on how emerging technologies—particularly AI and generative AI—are reshaping state-citizen relations. While digital tools promise more efficient public services, their deployment often lacks adequate safeguards, raising concerns about privacy, accountability, and civil liberties. Drawing on the concept of Surveillance Developmentalism, the paper argues that Southeast Asian states increasingly use digital infrastructure for control under the guise of progress. Case studies from Thailand and Myanmar illustrate how data collection, algorithmic systems, and weak oversight can marginalize communities and entrench asymmetries of power. The paper calls for a shift toward rights-based digital governance that prioritizes transparency, community participation, and data justice. It concludes with policy recommendations to mandate privacy-by-design, enhance digital literacy, and establish participatory oversight mechanisms. Without ethical guardrails, digital development risks exacerbating existing inequalities rather than delivering inclusive progress.

Introduction

Digital technologies, particularly artificial intelligence and generative AI (GenAI), are reshaping the landscape of global development. From optimizing social protection systems to enhancing smart infrastructure in cities, these innovations promise more inclusive and efficient governance. Yet, their increasing reliance on data, often extracted without full understanding or consent, raises profound ethical and legal questions about privacy, surveillance, and power. This reflection treats AI development as a subset of digital development sought after by state actors as it explores how development agendas can responsibly harness emerging technologies while protecting the fundamental rights of individuals, especially in underregulated or vulnerable contexts. Drawing on the frameworks of surveillance capitalism and Southeast Asian experiences, it argues for a shift toward rights-based, people-centric governance that embeds accountability and community agency at its core.

While surveillance capitalism, as articulated by Shoshana Zuboff, was originally developed to critique how private corporations extract personal data for behavioral prediction and profit, its core dynamics; namely, data capture, asymmetrical power, and opacity, are increasingly mirrored in state-led digital development programs. In Southeast Asia, governments and their development partners increasingly deploy artificial intelligence and big data tools under the banner of national progress, digital transformation, or efficient service delivery. These interventions often collect granular data on citizens, ranging from biometric IDs and health records to digital transactions and mobility patterns, with little meaningful consent from citizens or measures for redress. Although the aim is not always commercial gain, this form of "surveillance for development" risks reproducing the same structural asymmetries Zuboff warns against: individuals as passive data sources, and institutions, whether private or public, as unaccountable stewards of that data.

Crucially, the power dynamic in state-led data extraction differs from corporate surveillance in that the state can exercise coercive authority over its population from mandating participation in digital ID systems, denying benefits for non-compliance, or using predictive algorithms in policing or welfare targeting. This renders the surveillance-development nexus even more consequential. When development agencies promote or fund such programs, often through "smart governance" or "digital inclusion" initiatives, they may inadvertently entrench what could be called Surveillance Developmentalism: the use of data-driven technologies to expand state capacity without adequate safeguards for civil liberties, data

justice, or marginalized populations. While private firms may be restrained by market pressure or regulation, state-led systems often operate under looser accountability regimes, especially in semi-authoritarian or hybrid regimes common in parts of Southeast Asia.

The Promise and Peril of Technologies in Development Agendas

In this era of digitalization and interconnectedness, emerging technologies, ranging from digital platforms to artificial intelligence, have become integral to development programs. Countries have sought to capitalise on the promised potential of technologies for more effective governance, from predictive analytics in public health to digital ID systems for aid delivery. In theory, these tools can promote efficiency, reduce leakage, and personalize services for marginalized populations. For example, machine learning models are being used to map out poverty hotspots while satellite imagery is used to develop Geographic Information System (GIS) to forecast agricultural yields for climate-vulnerable communities in developing countries, such as Thailand and India (Asian Development Bank (ADB) 2021; Gulecha and Reshmi 2024; Xie et al. 2016). Agentic and predictive AI tools have been introduced to streamline data processing and minimizing human errors in multiple sectors, including healthcare and defence. However, these benefits can mask a darker reality: development initiatives often collect vast amounts of personal and biometric data with limited oversight. As Zuboff (2019) explains in her theory of surveillance capitalism that socioeconomic and personal data can be repurposed for profit or political control, transforming individuals into "data subjects" rather than empowered citizens. While surveillance capitalism focuses on the entrenched data collection done by digital platforms for profit-oriented goals, it can also be extended to produce a more robust understanding about public-private collusion in the digital sphere. On one hand, the co-optation between the big tech companies as suppliers of data and sovereign states as users of data can result in development projects that serve as testing grounds for surveillance tools. On the other hand, it means that states have relatively low incentives to reign in platforms' broad public surveillance capabilities despite it being an invasion of privacy to users who do not want their private experience to be owned by a company.

In Southeast Asia, a complex relationship between digital development, internet freedom, and state control often reflects a global trend towards reduced internet freedom despite advancements in digital infrastructure. Many countries in Southeast Asia have made significant progress in developing their digital infrastructure and implementing e-

government services, with the region's E-government Development Index (EDGI) in 2022 being higher than the world average. However, this bolstered digital capacity also serves as an instrument for state repression, infringing on citizens' rights.

Over the past decade, most Southeast Asian countries have bolstered their capabilities for digital repression. The emergence of social media as a tool for social movements, exemplified by the Arab Spring and Thailand's PDRC protest, has incentivised the enhancement of these infrastructural controls. According to Sriyai's study (2024b), this increase is particularly notable in their capacity to control digital infrastructure through Internet filtering capability, Internet shutdown capability, and social media monitoring capability. Interestingly, there is no discernible divide in this capacity between high-income and low-income countries or different regime types. For example, Myanmar, the poorest ASEAN country, has similar internet filtering and shutdown capabilities to Singapore, the region's richest, and even surpasses Singapore in social media monitoring capability. This suggests a "need-based" logic, where political control and survival drive states to build capacity in anticipation of security threats. Moreover, most countries tend to avoid broad-based tactics like internet shutdowns or blocking all websites, despite having the capacity to do so. This is due to significant socioeconomic trade-offs, including the risk of losing economic productivity and increasing social tension. As such, governments generally prefer "softer, more imperceptible approaches (Sriyai 2024b, 9)", such as social media surveillance and censorship, for infrastructural control.

Privacy Risks and Legal-Policy Gaps

The proliferation of emerging technologies, particularly AI tools, in development often outpaces the legal safeguards necessary to regulate them. As mentioned in the previous section, Southeast Asian countries leverage their advanced digital capabilities for both development and control. While building robust infrastructural control capacities and technological advancement, they often exercise these powers selectively. The UN Trade and Development (UNCTAD)(2025) shows that 75 per cent of countries had some data protection and privacy legislation (commonly known as PDPA Law) by 2021. Yet, governments worldwide have been under pressure over concerns about data protection and the privacy of their citizens. While frameworks like the EU's *General Data Protection Regulation (GDPR)* (2016) can be used as a baseline reference of a global standard, many low- and middle-income countries lack robust data protection laws, institutional capacity, or leverage to enforce them. This legal vacuum, then, creates space for excessive data

collection, long-term storage of sensitive information, and potential abuses under the banner of "development." Moreover, fragmented policy environments often leave citizens without clear mechanisms for redress or consent.

A case in point is Thailand. As the country is embracing artificial intelligence (AI) with great enthusiasm, viewing it as a catalyst for economic growth and digital transformation, Thailand's domestic frameworks to regulate digital development have left much to be desired. For instance, the country's enforcement of the Personal Data Protection Act (PDPA) of 2019 has proven to be light-handed when the violations stemmed from the public sector (Sriyai 2024a). In his statement, the minister for Digital Economy and Society admitted that an extensive review of 31,561 state-run units from November 2023 to late August 2024 revealed 6,086 instances of personal data breaches, with local administrative organisations as the primary culprits (Tantivangphaisal 2024). In an earlier case, data was leaked from the Department of Older Persons, exposing 20 million Thais to potential cyber threats and scams. They also found 139 incidents where officials illicitly sold citizens' personal data though the minister did not disclose how many citizens could potentially be affected by these incidents (Sriyai 2024c). Most astoundingly, there has yet to be any news about how these cases are being investigated and whether any individuals have been held responsible for the leaks of citizens' personal data, raising suspicion of the government's willingness to admit its own faults and provide redress to the affected citizens. Considering this, it remains doubtful whether the authorities are prepared to apply the law equally when data theft or breaches involve the public sector, which raises concerns about cybersecurity in state-driven development initiatives.

More specifically on AI development, the National AI Action Plan (2022–2030) outlines Thailand's strategies to integrate AI into sectors like healthcare, agriculture, and tourism, aiming to enhance competitiveness and reduce reliance on foreign technology (Trisadikoon and Umponkitviwat 2025). However, as the nation accelerates AI adoption in hope to unleash AI's economic promises, it is seemingly falling behind on the equally urgent task of developing sufficient AI governance measures, particularly in the realm of generative AI (GenAI), which will be discussed in greater detail in the forthcoming section.

While Thailand's case of enforcement lapses underscores the reality of many low- and middle-income countries in Southeast Asia and elsewhere, a case in which policy and related programs are being deliberately used to enhance the state's surveillance capabilities is Myanmar. There, the surveillance efforts are often presented under the guise of broader development agendas and public service initiatives. This strategy allows the military junta to

bolster its digital control while maintaining a veneer of progress and national improvement. In September 2022, the Ministry of Transport and Communications publicly announced the completion of digitization and registration of 52 million people using 'e-ID Biographic Registration Software' technology, forming a national database. This public declaration of a national database can be framed as a step towards digital development and efficient data management; especially when combined with its prior requirement on mandatory sim card registration that began in 2016 (The Arakan Express News 2022). The 'e-ID' project gained more momentum in 2023, with the State Administration Council (SAC) announcing plans for biometric data collection in Naypyidaw. The subsequent mandatory requirement of UID for local travel, passport applications, and Temporary Border Passes (TBP) forced mass biometric data collection, which was then used to identify, track, and arrest dissidents, according to the report by Myanmar Internet Project (2025).

The same report also highlights the weaponization of "Safe City, Smart City" Initiatives by the military government. With the technical support from China, the junta later rapidly expanded the CCTV networks that were initially installed in major cities such as Mandalay, Yangon, and Naypyidaw as part of "Safe City, Smart City" initiatives under the civilian government. Although these initiatives are often promoted as urban development projects aimed at improving public safety and efficiency, the CCTVs are presumed to be integrated into technologies like the PSMS (Person Scrutiny and Monitoring System), enabling blanket surveillance and allowing for monitoring and tracking of targeted individuals. Neighboring countries, and even the regional body like ASEAN, has not reacted to this overt surveillance of citizens in Myanmar as they view it as domestic affairs, illustrating the bloc's emphasis on non-interference principle.

Governance and Ethics

To ensure ethical implementation, emerging technologies, including AI tools, used in development must be transparent, auditable, and built with safeguards against bias. The integration of generative AI (GenAI) into development communications and planning is reshaping how narratives are framed, decisions are modeled, and resources are prioritized. In programmatic communications, GenAI tools can rapidly generate reports, impact stories, policy briefs, and community profiles, ostensibly enhancing efficiency. Yet this automation also raises epistemic risks: whose voice is being amplified, which data informs the narrative, and what local contexts may be flattened or misrepresented in the process? As development institutions and governments increasingly experiment with GenAI for scenario modeling or

needs assessments, there is a risk that AI-generated content may subtly guide policy directions or resource allocation without adequate scrutiny or local validation.

When GenAI systems generate policy recommendations, funding priorities, or targeting models, the opacity of their training data and algorithms can obscure embedded biases, political assumptions, or methodological flaws. In practice, this could result in skewed prioritization. More importantly, the affected communities may lack the technical or institutional means to identify, question, or contest these AI-generated proposals, particularly when wrapped in technocratic language. Without transparent documentation of how GenAI outputs are produced, and without clear pathways for community feedback or correction, these tools risk disempowering the very populations development aims to serve.

This section uses Thailand's attempts to incorporate and govern emerging technologies in its development initiatives as illustrative cases as to why development agendas need to be grounded in the principle of transparency, accountability, and explainability.

As it stands, Thailand's current approach on AI governance, while influenced by the EU's *AI Act*, lacks the same depth and enforceability concerning GenAI. Under Article 52 of the Act, the EU requires that any content generated or manipulated using AI, be it deepfake images, audio, or video, must include clear, visible labelling to inform users that the content is artificially produced. Deployers of GenAI systems are also expected to disclose AI involvement and apply technical safeguards to embed traceability into AI-generated content (European Parliament 2023). On the other hand, Thai legislation does not include any requirement for clear labelling of GenAI-generated content. There are no mandates for transparency or traceability, and in this manner, the burden of detection often falls to users, journalists, or civil society, who lack the tools and resources necessary to respond at scale.

Equally important is the role of social media platforms, which serve as primary channels for the distribution of GenAI content. The UK's *Online Safety Act of 2023* exemplifies a state's attempt to hold platforms at a higher standard of responsibility in moderating manipulated media. Algorithms that amplify engagement over accuracy can accelerate the spread of misinformation; thus, platforms should be required to disclose when and how AI is used in content generation or recommendation engines, and to deploy detection tools that identify and flag inauthentic content in real-time (Richards 2025). Greater transparency through regular audits and clearer content labelling would help restore public trust and support efforts to build a safer digital environment. Overall, the absence of explicit provisions on

platforms' accountability from Thailand's drafted legislations leaves a regulatory gap that could be exploited, undermining public confidence and safety.

At this stage, it remains unclear how the Thai government and relevant state agencies are planning to incorporate GenAI into policymaking. The lack of clarity in this aspect should also be a red flag. During a field research project in Northern Thailand, it was observed that a development project aimed at optimizing agricultural productivity through satellite-based data collection unintentionally marginalized highland communities. Local farmers, many of whom were older ethnic minorities, had little understanding of how their planting cycles, land use, or biometric data were being digitized and fed into predictive models. These models, then, are intended to be used by local authorities to determine the farmers' land use and land allocation. As a result, some highland communities ended up being told to grow crops in ways that are against their indigenous practices and knowledge. While the intentions were good, the implementation lacked consultation and feedback loops, reinforcing what Mejias and Couldry (2024) describe as "data colonialism"— a renewed effort to seize valuable resources for the benefit of elites based on the extraction and appropriation. In this era, one of the most high-value commodities is data and this local experience reiterates how, without ethical and participatory safeguards, even a well-meaning innovation can replicate extractive dynamics and cause tension between state and citizens.

The inclusion of affected communities in the design, implementation, and governance of digital development is critical for trust and legitimacy. Public participation not only democratizes decision-making but also surfaces cultural, contextual, and ethical concerns that designers or policymakers might overlook. Informed consent should go beyond checkbox compliance: it must be meaningful, accessible, and ongoing.

Discussion

In the pursuit of inclusive digital development, we must not trade rights for convenience and efficiency. Emerging technologies, when governed properly, can offer transformative solutions, but its risks must be openly acknowledged and mitigated. Embedding privacy by design, fostering digital literacy, and grounding governance in justice-based principles are essential. Specifically, countries should consider the following points as they proceed with their digital development agenda.

To operationalize ethical AI governance in development contexts, abstract principles such as privacy, participation, and accountability must be translated into measurable outcomes.

Privacy protection, for example, can be demonstrated through data minimization practices, regular third-party audits, and transparent consent mechanisms that allow individuals; especially those with low digital literacy, to meaningfully control how their data is used. Effective grievance redress systems that track and resolve privacy-related complaints also serve as critical accountability tools. Meaningful community participation can be assessed by the degree to which marginalized groups are represented in AI policy design and decision-making processes. Evidence that AI systems are advancing development rather than enabling surveillance can be seen in whether their outputs correlate with more equitable service delivery, improved welfare targeting, or reductions in bias across socioeconomic and demographic lines. Transparency and oversight are key: indicators such as the publication of model documentation, the frequency of fairness audits, and the existence of independent bodies empowered to review or halt deployments are essential to ensuring that AI supports development goals while respecting human rights.

Mandate Privacy-by-Design in All Public Digital Infrastructure

Governments must require that all digital systems, particularly those used in public service delivery, welfare targeting, or digital identification, embed privacy-by-design principles from the outset. This involves minimizing the collection of personal data, ensuring that only relevant information is gathered and retained for a limited period, and that systems are built with user consent, purpose limitation, and data security as default settings. Public digital platforms should incorporate transparent data governance policies, privacy impact assessments, and clear channels for grievance redress. By making privacy an architectural cornerstone rather than an afterthought, states can protect individuals from surveillance overreach and build long-term public trust in digital transformation initiatives.

To note, this recommendation may face significant political economy challenges, particularly in contexts where state institutions may benefit from opaque data practices or where surveillance aligns with broader security or control agendas. Government compliance cannot be assumed, especially when data centralization serves political or bureaucratic interests. To shift incentives, compliance could be tied to funding or technical assistance from international development agencies, many of which now include digital safeguards in their governance frameworks. Oversight mechanisms should include independent data protection authorities with enforcement power, backed by legislation that mandates privacy impact assessments and routine audits for all new digital infrastructure projects. Civil society organizations (CSOs) can monitor implementation by engaging in technology assessments,

pushing for public reporting requirements, and building alliances with investigative media or legal advocacy groups to expose non-compliance. Internationally, trade agreements, aid conditionalities, or digital governance partnerships can apply pressure by tying collaboration to data protection standards. A partnership between EU and ASEAN should be considered and explored. However, this requires sustained transnational civil society engagement to ensure such standards are not only adopted but meaningfully implemented on the ground.

Invest in Community-Based Digital Literacy Programs

Closing the digital divide requires more than expanding internet access. It demands a focus on digital literacy that is locally grounded, culturally sensitive, and critically aware. Governments and development agencies should invest in community-based programs that go beyond technical skills to include topics such as online safety, recognizing misinformation, protecting personal data, and understanding one's digital rights. Public-private partnerships in this aspect should also be explored since the private sector is generally more well-equipped than the public sector in terms of both technical and financial resources to carry out the programs. These efforts should be especially prioritized for vulnerable populations, such as rural residents, women, the elderly, informal workers, and displaced persons, who often face the highest exposure to digital threats but the least protection. Equipping citizens with the capacity to engage critically and safely in the digital world is crucial not only for empowerment, but for reducing susceptibility to online scams, exploitation, and misinformation.

Establish Transparent and Participatory Tech Governance Frameworks

To ensure that digital development is inclusive, ethical, and accountable, states should establish governance frameworks that are both transparent and participatory. This means creating multi-stakeholder oversight bodies that include civil society organizations, legal experts, technologists, representatives from marginalized communities, and human rights defenders. These bodies should have meaningful authority to assess and oversee the design, procurement, and deployment of AI and digital systems, particularly those with surveillance capabilities or affecting public services. They should have legal authority to halt or delay the deployment of AI and digital systems that fail to meet human rights, privacy, or equity benchmarks. They must be granted budgetary oversight of AI procurement and implementation, allowing them to scrutinize contracts, assess vendor accountability, and

ensure that procurement aligns with public interest goals. Additionally, subpoena power to access internal government documents, algorithmic design records, and risk assessments is essential to penetrate the opacity that often surrounds partnerships between state and tech entities. Mandatory public hearings and consultation processes should be built into system design and deployment cycles, especially when technologies impact vulnerable groups. To prevent capture by well-resourced corporate or political actors, these governance bodies must be structurally independent, with multi-stakeholder representation, term limits, and stringent conflict-of-interest rules.

Strengthen National Cybersecurity Safeguards

As digital platforms proliferate across development sectors, from smart farming to health data systems, states must dramatically improve their cybersecurity posture to prevent malicious actors from exploiting weak infrastructure. This includes developing national cybersecurity strategies, investing in cyber defense capabilities, and establishing dedicated institutions or units to oversee risk monitoring and incident response. All public-facing systems, especially those handling sensitive personal data, should undergo regular security audits and vulnerability assessments. States should also foster regional and international cooperation to address transnational cyber threats and ensure that platforms operating across borders adhere to shared security and privacy standards. In fact, ASEAN as a regional body has made strides in developing common principles for governance of digital development. For instance, *Framework on Personal Data Protection* (2016) and the *Framework on Digital Data Governance* (2018) that were endorsed at the ASEAN Telecommunications and Information Technology Ministers Meetings serve as a promising pathway for discussions about regional standard while the *ASEAN Guide on AI Governance and Ethics* (2024) and its *Expanded Guide on Gen AI* (2025) have provided some meaningful recommendations to be considered by Member States as guidelines for their digital development agenda.

References

ASEAN Secretariat. 2016. "FRAMEWORK ON PERSONAL DATA PROTECTION." *ASEAN TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY MINISTERS MEETING (TELMIN)*: 1–6.

ASEAN Secretariat. 2018. "FRAMEWORK ON DIGITAL DATA GOVERNANCE." *ASEAN TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY MINISTERS MEETING (TELMIN)*: 1–9.

ASEAN Secretariat. 2024. *ASEAN Guide on AI Governance and Ethics*.

ASEAN Secretariat. 2025. *Expanded ASEAN Guide on AI Governance and Ethics--Generative AI*. https://asean.org/wp-content/uploads/2025/01/Expanded-ASEAN-Guide-on-AI-Governance-and-Ethics-Generative-AI.pdf (July 1, 2025).

Asian Development Bank (ADB). 2021. *MAPPING THE SPATIAL DISTRIBUTION OF POVERTY USING SATELLITE IMAGERY IN THAILAND*. Manila. doi:10.22617/TCS210112-2.

European Parliament. 2023. "EU AI Act: First Regulation on Artificial Intelligence." *European Parliament*. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence (July 1, 2025).

European Union. 2016. *General Data Protection Regulation (GDPR)*. European Union.

Gulecha, Srishti R, and Muthu K Reshmi. 2024. "Poverty Mapping in India Using Machine Learning and Deep Learning Techniques." *ISPRS Annals of the Photogrammetry, Remote Sensing and Spatial Information Sciences* X-4–2024: 319–26. doi:10.5194/isprs-annals-X-4-2024-319-2024.

Mejias, Ulises Ali., and Nick. Couldry. 2024. *Data Grab: The New Colonialism of Big Tech and How to Fight Back*. The University of Chicago Press.

Richards, Anna. 2025. "Online Safety Act: Privacy Threats and Free Speech Risks." *The Constitution Society*. https://consoc.org.uk/the-online-safety-act-privacy-threats-and-free-speech-risks/ (May 26, 2025).

Sriyai, Surachanee. 2024a. "Data Leaks: Thai Government Tough on Private Firms, Soft on Public Sector and Cybercriminals | FULCRUM." *Fulcrum*. https://fulcrum.sg/data-leaks-

thai-government-tough-on-private-firms-soft-on-public-sector-and-cybercriminals/ (June 30, 2025).

Sriyai, Surachanee. 2024b. "How Means for Digital Repression in Southeast Asia Have Unfolded in Recent Times." *Pespective* 2024(65): 1–12. https://www.iseas.edu.sg/wp-content/uploads/2024/08/ISEAS_Perspective_2024_65.pdf (June 30, 2025).

Sriyai, Surachanee. 2024c. "Thailand's Public Sector Data Breaches Erode Public Trust – And Might Undermine E-Government | FULCRUM." *Fulcrum*. https://fulcrum.sg/thailands-public-sector-data-breaches-erode-public-trust-and-might-undermine-e-government/ (July 1, 2025).

SRS. 2025. "Myanmar Military Junta's Increasingly Powerful Surveillance Ecosystem Over Four Years." *Myanmar Internet Project*. https://www.myanmarinternet.info/post/surveillance_ecosystem_over_four_years-1 (July 1, 2025).

Tantivangphaisal, Puntid. 2024. "Local Thai Agencies Blamed for Majority of State Data Breaches" *Thaiger*. https://thethaiger.com/news/national/thai-local-agencies-blamed-for-majority-of-state-data-breaches (July 1, 2025).

The Arakan Express News. 2022. "စစ်ကောင်စီမှ ဖုန်း SIM Card များ မှတ်ပုံတင်ခြင်းကို ပြန်လည်စစ်ဆေးမည်ဟု ကြေညာ ." *Facebook*. https://www.facebook.com/100077838627276/posts/pfbid02JNNkGNQsgEi6WsA4tGHUoR7ehGA3pDJ1QUZD48QuEgyRqWXirLGXpf5V21JYTHxtl/ (July 1, 2025).

Trisadikoon, Khemmapat, and Wichayada Umponkitviwat. 2025. "Navigating Thailand's AI Law: Development at a Crossroads." *Tech For Good Institute*. https://techforgoodinstitute.org/blog/expert-opinion/navigating-thailands-ai-law-development-at-a-crossroads/ (July 1, 2025).

UN Trade and Development (UNCTAD). 2025. "Data Protection and Privacy Legislation Worldwide." *UN Trade and Development (UNCTAD)*. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (July 1, 2025).

Xie, Michael, Neal Jean, Marshall Burke, David Lobell, and Stefano Ermon. 2016. "Transfer Learning from Deep Features for Remote Sensing and Poverty Mapping." *Proceedings of the AAAI Conference on Artificial Intelligence* 30(1): 3929–35. doi:10.1609/AAAI.V30I1.9906.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, NY: PublicAffairs.

INFORMATION RESILIENCE & INTEGRITY SYMPOSIUM

Generative AI and Information Resilience in the Asia-Pacific: Actions and Adaptations

Faculty of Social and Political Sciences
Universitas Gadjah Mada

21 August 2025

saferinternetlab.org/iris @saferinetlab @cfds_ugm iris@saferinternetlab.org