ACT
Association for
Competitive Technology

31 August 2026

Ir. Dr. Megat Zuhairy bin Megat Tajuddin
Chief Executive
National Cyber Security Agency (NACSA)
National Security Council
Prime Minister's Department
Level LG & G, West Wing, Perdana Putra Building
Federal Government Administrative Centre
62502 Putrajaya
Malaysia

cc: YAB Datuk Seri Dr Ahmad Zahid Hamidi, Deputy Prime Minister
Attorney General's Chambers of Malaysia
Malaysian Communications and Multimedia Commission

RE: Implementation of the Cybercrimes Bill 2026

The Association for Competitive Technology (ACT) writes regarding the implementation of the Cybercrimes Bill 2026, which passed the Dewan Rakyat on 1 July 2026 and the Dewan Negara on 20 July 2026 and now awaits Royal Assent, gazettal, and a commencement order.[1] ACT supports Malaysia's objective of modernising a framework that has rested on the Computer Crimes Act 1997 for nearly three decades, and we recognise the Government's intention to align that framework with the United Nations Convention against Cybercrime, which Malaysia signed at the Hanoi signing ceremony in October 2025, and with the Council of Europe Convention on Cybercrime, to which Malaysia has been invited to accede.[2] We write about the clauses that bear on commercial encryption and on the ability of micro, small, and medium-sized enterprises (MSMEs) to protect the data they hold for users, and to offer recommendations on the guidance and administrative practice that will determine how those clauses operate once the Act commences.

[1] The Cybercrimes Bill 2026 was tabled for first reading in the Dewan Rakyat on 22 June 2026, passed the Dewan Rakyat on 1 July 2026, and passed the Dewan Negara on 20 July 2026. Clause 1 provides that the Act comes into operation on a date appointed by the Minister by notification in the Gazette. Text of the Bill at https://www.msc.com.my/cyberlaws/CYBERCRIMES-BILL-2026.pdf. See also Skrine, The Cybercrimes Bill 2026 – Update (23 July 2026), https://www.skrine.com/insights/alerts/july-2026/the-cybercrimes-bill-2026-update.

[2] Malaysia signed the United Nations Convention against Cybercrime at the opening for signature in Hanoi on 25 October 2025. United Nations Office of Legal Affairs, https://www.un.org/ola/en/news/united-nations-convention-against-cybercrime-opens-signature-hanoi. Malaysia is an observer to the Council of Europe Convention on Cybercrime and has been invited to accede. Council of Europe, Parties and Observers to the Budapest Convention, https://www.coe.int/en/web/cybercrime/parties-observers. The Government stated its intention to accede in the Dewan Rakyat on 23 July 2025. The Star, 23 July 2025, https://www.thestar.com.my/news/nation/2025/07/23/m039sia-to-sign-un-convention-on-cybercrime-in-october-dewan-rakyat-told.

I. Statement of Interest

ACT represents the global small business technology developer community, including developers and connected device companies across the Asia-Pacific region. Our members are MSMEs. They write the software that runs on smartphones, in vehicles, in clinics, in warehouses, and in the systems that merchants and service providers depend on. They use commercial encryption, including end-to-end encryption where the architecture of the service calls for it, to protect financial data, health information, authentication credentials, and other sensitive material that users entrust to them.

That position gives ACT members a particular stake in how clauses 36, 38 to 41, 51, and 52 are administered. They have no in-house security counsel and no government affairs teams, and they cannot redesign cryptographic architecture country by country. Where a decryption or interception obligation is drafted as though every provider holds plaintext or keys, a firm that holds neither is left to choose between leaving the market and rebuilding its product in a way that lowers security for every user of that product, in Malaysia and everywhere else. Encryption is how an MSME earns the trust that lets it compete, and the way these clauses are administered will decide whether MSMEs can continue to serve Malaysian users.

ACT has engaged Malaysian and regional policymakers on adjacent questions, including comments to the Malaysia Competition Commission on its market review of the digital economy ecosystem in September 2025[3] and recommendations on the ASEAN Digital Economy Framework Agreement ahead of the 47th ASEAN Summit in October 2025, which asked that the framework preserve the ability to use technical protection mechanisms, including commercial encryption, to secure data transactions.[4] We ask the Agency to keep MSME developers in view as it prepares for commencement.

II. General Views

ACT offers the following general views on how cybercrime rules that touch encryption should be administered:

- **Encryption is a vital measure MSMEs rely on.** Encryption is how MSME developers protect payments, health data, credentials, and intellectual property, and how networks and platforms resist the class of intrusion that the Cyber Security Act 2024 and the Malaysia Cyber Security Strategy 2025–2030 were built to address. Treating a provider's inability to produce plaintext as obstruction under clause 46 would work against both.
- **Exceptional access cannot be confined to its intended user.** A capability built so that an authorised officer can obtain decrypted content is available to anyone who finds it or who

[3] Association for Competitive Technology, Comments to the Malaysia Competition Commission on the Public Consultation of the Draft Final Report for the Market Review of the Digital Economy Ecosystem under the Competition Act 2010 (14 September 2025), https://actonline.org/wp-content/uploads/2026/06/ACT-Comments-re-Final-Draft-Market-Review-of-the-Digital-Economy-Ecosystem-Report-14-Sept-2025.pdf.

[4] Association for Competitive Technology, Recommendations Supporting the Development of the ASEAN Digital Economy Framework at the 47th Annual ASEAN Summit (28 October 2025) ("Preserve the ability to use technical protection mechanisms, including commercial encryption, to secure data transactions"), https://actonline.org/post/act-the-app-association-recommendations-supporting-the-development-of-the-association-of-southeast-asian-nations-asean-digital-economy-framework-at-the-47th-annual-asean-summit/.

can compel its use. In the Salt Typhoon intrusions, the FBI and CISA confirmed that a state-sponsored actor copied information subject to United States law enforcement requests made under court orders.[5] The Global Statement on Encryption, which ACT convened and 61 organisations co-signed in November 2025, makes the same point about backdoors, key escrow, and technical mandates.[6]

- **A provider can produce only what it holds.** Where a service is designed so that keys and plaintext remain on the endpoints, the provider cannot decrypt the traffic. Guidance that treats that design as non-compliance does not produce evidence. What it produces is a decision inside the firm to block Malaysian users, or to ship a less secure product everywhere.
- **Lawful investigation does not depend on weakening encryption.** ACT recognises that law enforcement and national security agencies have legitimate evidentiary needs. Those needs are met by targeted legal process directed at parties who hold the data sought, and by the investigative powers clauses 45, 47, and 48 already confer. They are not met by asking every MSME developer with a Malaysian user to re-engineer its encryption.
- **Clause 52 indicates that Parliament did not intend a content storage mandate.** The retention power in clause 52 is confined to computer data other than content data and is conditioned on national security or public safety necessity and on proportionality. Guidance under clauses 40, 41, and 51 should be read consistently with that limit rather than as a route around it.
- **Administration should sit alongside Malaysia's own cryptography policy.** The Cabinet approved MyKriptografi, the successor to the 2013 National Cryptography Policy, on 28 November 2025 as a framework for strengthening cryptographic governance and protecting the data of government, industry, and citizens.[7] Practice under the Cybercrimes Act should be consistent with it.
- **Extra-territorial reach should remain workable for MSMEs.** Clause 2 applies the Act to any person of any nationality where the computer system or data was in Malaysia, was connected to a Malaysian system, or where the affected person is Malaysian. Large operators can typically staff for that exposure. An MSME cannot. Guidance should say how an MSME outside Malaysia, with no establishment in Malaysia and no keys to end-to-end encrypted traffic, is expected to respond to a notice.
- **The security controls MSMEs depend on should be preserved.** MSMEs build on distribution and infrastructure services — app marketplaces, cloud hosting and platform services, payment processing, and identity and fraud-prevention providers — that provide

[5] Joint Statement from the FBI and CISA on the People's Republic of China Targeting of Commercial Telecommunications Infrastructure (13 November 2024), confirming among other things the copying of certain information that was subject to United States law enforcement requests pursuant to court orders, https://www.fbi.gov/news/press-releases/joint-statement-from-fbi-and-cisa-on-the-peoples-republic-of-china-targeting-of-commercial-telecommunications-infrastructure.

[6] Global Statement on the Role of Encryption in Securing Trust and Enabling the Digital Economy (17 November 2025) ("Any effort to undermine encryption, whether through backdoors, key escrow systems, or technical mandates, undermines that trust."), https://actonline.org/wp-content/uploads/2026/06/global_statement_on_the_role_of_encryption_in_securing_trust_and_enabling_the_digital_economy__nov_2025_.pdf.

[7] National Cyber Security Agency, MyKriptografi – National Cryptography Policy, approved by the Cabinet on 28 November 2025, available at https://www.nacsa.gov.my/kriptografi-view.php.

security review, fraud screening, and integrity controls. Nothing in implementation should require those providers to reduce those controls, to distribute software that has not been reviewed, or to disable encryption in order to satisfy a duty under clauses 40, 41, or 51.

- **Cross-border data movement depends on encryption remaining usable.** MSMEs move data because their users and suppliers are not confined to one country. A decryption or storage requirement that can be met only by breaking end-to-end encryption works in practice as a localisation or exit requirement. Keeping encryption intact is the lower-friction way to keep Malaysian users on the same secure products users elsewhere already have.
- **Broad data-access readings should not displace encryption or the PDPA.** Readings that would call for continuous, real-time, or non-aggregated access to third-party content sit awkwardly beside the Personal Data Protection Act 2010 and the security obligations Malaysian businesses already carry.

III. Comments on Implementation

Parliament has adopted the Bill, and ACT does not ask the Agency to revisit it. We ask that the following be settled in the commencement order, in officer guidance, and in the notice practice the Agency develops with the Attorney General's Chambers and MCMC.

- **Clause 36 should not be administered as a duty to build exceptional access.** Clause 36 lets an authorised officer conducting a search demand passwords, decryption codes, and the software or hardware needed to read the information, with non-compliance reaching the obstruction offence in clause 46 and its fine of up to RM100,000 or three years' imprisonment.[8] ACT asks for three clarifications, none of which would require amending the Act:[9]
    - A demand under clause 36 reaches only material the recipient actually possesses or controls.
    - A provider that holds no plaintext or keys for an end-to-end encrypted service does not obstruct an investigation by saying so.
    - Clause 36 does not require anyone to build a decryption capability, a key escrow arrangement, or any other form of exceptional access into a product.
- **Preservation, disclosure, and interception duties should track what a provider holds.** Clauses 38 and 39 let an authorised officer require preservation and disclosure of computer data. Clauses 40 and 41 let the Public Prosecutor require real-time traffic data collection and interception of content data, and both confine that requirement to the service provider's

[8] Cybercrimes Bill 2026, clauses 36 and 46, https://www.msc.com.my/cyberlaws/CYBERCRIMES-BILL-2026.pdf.
[9] Winding up debate on the Bill, the Deputy Prime Minister said of preservation notices that "the scope is limited only to the specific data identified in the notice issued" and that it is "not a blanket power to access an entire computer system or all of a person's information". New Straits Times, 1 July 2026, https://www.nst.com.my/news/nation/2026/07/1477937/dewan-rakyat-passes-cybercrimes-bill-2026-watch. He added that disclosure of computer data may be carried out only through a written notice to the person who owns or has control of the data, subject to the requirements of a lawful investigation. Bernama, 1 July 2026, https://www.bernama.com/en/general/news.php?id=2575501.

existing technical capability.[10] Guidance should give those words their plain meaning. Targeted process reaches content a service stores in recoverable form. It cannot reach content on an end-to-end encrypted service, because there is no such capability to exercise. Where the Act leaves room, the Agency and the Attorney General's Chambers should route interception and disclosure through prior independent authorisation, consistent with Article 24 of the Convention.[11]

- **Guidance should provide a way to report that compliance is technically impossible.** MSME developers will receive notices they cannot fulfil. Guidance should let a recipient certify, briefly and on the record, that it does not hold the plaintext, key, or capability sought, without that certification counting as obstruction under clause 46 or non-compliance under clause 51(3). Otherwise, the first such notice a five-person firm receives will read inside the firm as a reason to geo-block Malaysia.
- **The clause 51 duty should be tied to what the provider controls.** Clause 51(1) requires service providers to take necessary measures to prevent their services being used to commit cybercrimes, and clause 51(3) punishes non-compliance with a clause 51(2) notice by up to RM1 million or 10 years' imprisonment. The Bill does not say what those measures are. Read as measures within the provider's existing technical control, the duty works. Read as a mandate to re-architect a product's security, it does not. Clause 51(2) already requires the officer to consult MCMC, so the two agencies could publish worked examples of what satisfies the duty and what does not. That would help our members far more than an open-ended obligation carrying the Act's highest penalties.
- **Clause 39 confidentiality should not cut an MSME off from legal advice.** Clause 39 bars a recipient from disclosing the existence or contents of a notice. A large operator's in-house counsel is already inside the notice. Read literally, clause 39 would stop an MSME without in-house counsel from taking outside advice on whether a notice is valid or how to answer it. Guidance should confirm that a recipient may consult counsel under the same confidentiality obligation.
- **Name a single lead for encryption-related notices and take technical input before commencement.** The Act spans NACSA, the Royal Malaysia Police, the Attorney General's Chambers, and MCMC. An MSME needs one lead authority, one form of notice, and one place to raise an inability to comply. ACT would welcome a technical session on officer guidance and notice practice, with MSME developers present, before the commencement date is fixed. MCMC's February 2026 consultation on the draft Risk Mitigation Code and Child Protection Code is a workable model.[12]

[10] Clause 40(1) requires a service provider to act "within the service provider's existing technical capabilities". Clause 41(1) requires a service provider to act "within the service provider's technical capability". https://www.msc.com.my/cyberlaws/CYBERCRIMES-BILL-2026.pdf.

[11] United Nations Convention against Cybercrime, Article 24 (conditions and safeguards), which asks States Parties to subject these powers to judicial or other independent review, to grounds justifying their application, to limits on scope and duration, and to the principle of proportionality. See also Article 6 (respect for human rights) and Article 23 (scope of procedural measures). Text of the Convention annexed to United Nations General Assembly Resolution A/RES/79/243, https://docs.un.org/en/A/RES/79/243.

[12] Malaysian Communications and Multimedia Commission, public consultation on the draft Risk Mitigation Code and the draft Child Protection Code under the Online Safety Act 2025, opened 12 February 2026, with submissions closing 13 March 2026. See https://www.thestar.com.my/news/nation/2026/02/12/mcmc-launches-public-consultation-on-online-safety-plan. The codes were issued on 22 May 2026 and took effect on 1 June 2026. See

IV. Conclusion

ACT shares the Agency's objective of a digital environment in which Malaysian users are protected from cybercrime and MSMEs can compete on the merits. Encryption is one of the principal means by which MSMEs deliver that. The choice now in front of the Agency is whether clauses 36 and 38 to 41 are administered against the data a provider actually holds, or against an assumption that every provider can read every communication that touches a Malaysian user.

ACT asks the Agency to confirm, in guidance and in notice practice, that a decryption demand reaches only material in the recipient's possession or control, that inability to decrypt end-to-end encrypted traffic is not obstruction, that interception and storage duties do not require disabling encryption or creating exceptional access, that a recipient may certify an inability to comply, that a recipient may take legal advice on a notice, and that industry including MSMEs is consulted before commencement. We would welcome the opportunity to discuss any of these points with the Agency and to make our members available for technical input.

Thank you for your consideration of these comments.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Chapin Gregor
Global Policy Counsel

Association for Competitive Technology (ACT)
1401 K St NW (Ste 501)
Washington, DC 20005
United States

https://www.allenandgledhill.com/perspectives/publications/bulletins-malaysia/2026/mcmc-issues-risk-mitigation-code-and-child-protection-code-under-the-online-safety-act-2025/.