NO. 2024-15, JANUARY 2025
ISSN: 2086-8154

Economic Research Institute for ASEAN and East Asia

Policy Brief

Harmonising ASEAN's Anti-spam Regulations: Strategies for Effective Cross-border Enforcement and Enhanced Regional Cooperation

Mahirah Mahusin and Hilmy Prilliadi

Key Messages:

- ASEAN should adopt an opt-in model across ASEAN Member States to enhance cross-border enforcement and to ensure consistency in spam legislation, aligning with global good practices.
- ASEAN Member States should leverage international agreements to improve cross-border enforcement, share best practices, and foster joint capacity building.
- Empowering consumers through education and clear opt-out mechanisms is vital for reducing spam-related risks.
- Investment in advanced spam-filtering technologies should be prioritised to stay ahead of evolving threats.
- A region-wide anti-spam guideline should be developed that promotes legislative consistency, imposes stronger penalties for non-compliance, and strengthens weaker national frameworks.

Spam remains a critical issue in the digital landscape, despite its slight global decline. In 2023, spam accounted for 45.6% of global emails and remains a major vector for malware and phishing attacks. Within ASEAN, spam-related issues challenge productivity, cybersecurity, and consumer protection. To address these challenges, ASEAN Member States have initiated various anti-spam measures, guided by regional frameworks such as the ASEAN Digital Masterplan 2025 *and the ASEAN–China Initiative on Enhancing Cooperation on E-commerce. However, the diversity of anti-spam legislation – particularly the variance between opt-in and opt-out models – complicates cross-border enforcement. This policy brief advocates for a harmonised approach to spam regulation, drawing on international best practices. Recommendations include adopting an opt-in model for better cross-border enforcement, strengthening consumer education, investing in advanced spam-filtering technologies, and enhancing regional cooperation through frameworks like the Regional Comprehensive Economic Partnership agreement and the ASEAN–Australia–New Zealand Free Trade Area to ensure consistency and effectiveness in combating spam across ASEAN.*

Unsolicited commercial electronic messages,[1] or 'spam', remains an issue despite its recent decline. In 2023, 45.6% of global emails were spam, down from 49.0% in 2022, yet email remained the primary vector for malware (92.4%) and phishing attacks (96.0%) (INTERPOL, 2020.[2] Ransomware, often delivered via spam, continues to cause significant economic losses, estimated at US$257 billion between 2012 and 2020. These losses negatively impacted productivity, e-commerce, and the information and communications technology (ICT) sector (Alazab and Broadhurst, 2015; Karim et al., 2019). Additionally, 'spim' – spam targeting instant messaging – has risen with the increased use of mobile devices, requiring robust security features in instant messaging platforms (Australian Institute of Criminology, 2010).

Effectively addressing the pervasive issue of spam requires a coordinated effort amongst several key actors. The Organisation for Economic Co-operation and Development (OECD) Anti-Spam Toolkit of Recommended Policies and Measures recognised stakeholders who take measures against spam, including governments, internet service providers (ISPs), the ICT community, expert organisations, and end-users (Internet Governance Forum, 2024). Figure 1 depicts key aspects where these actors can contribute to reducing the impact of spam.

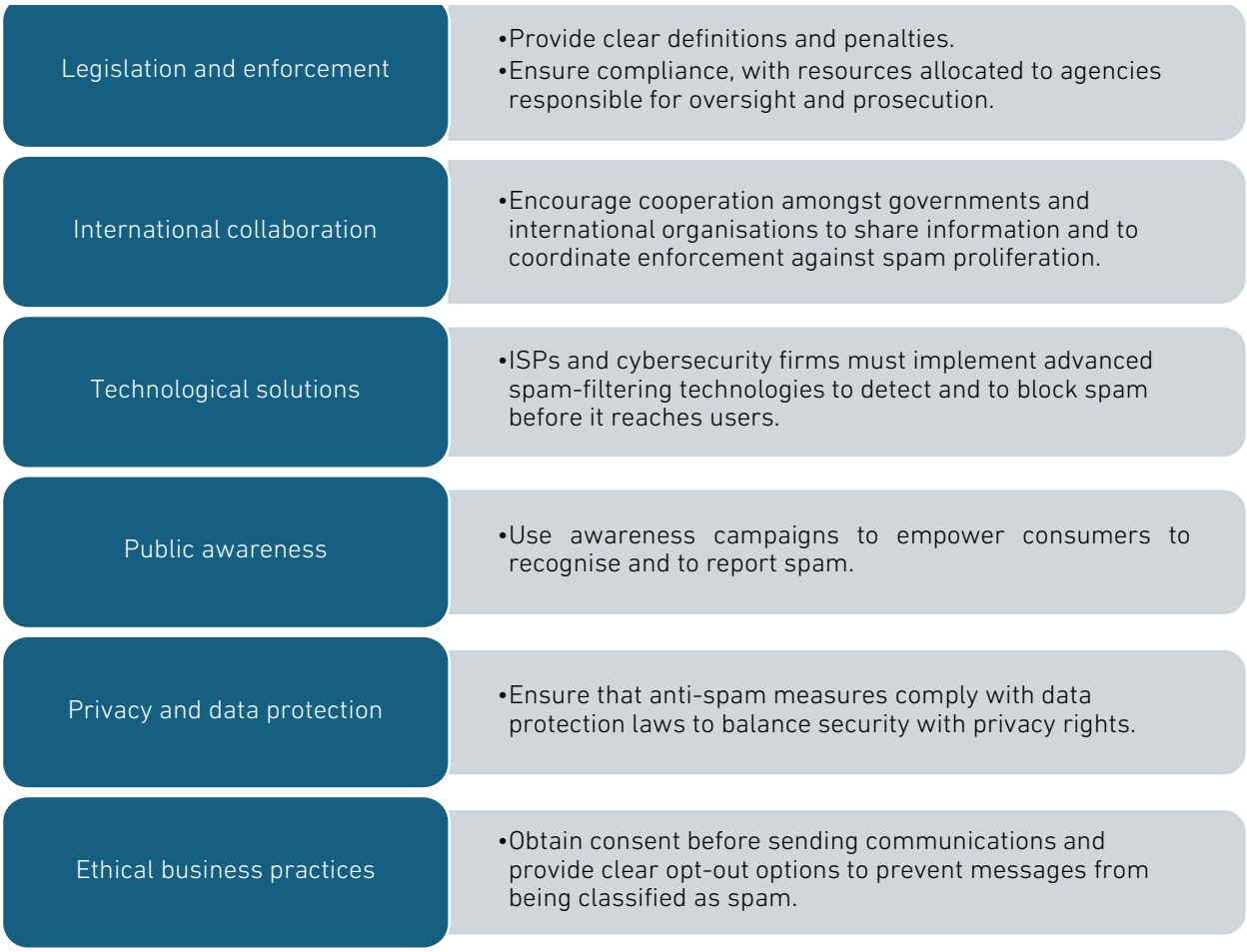
Mahirah Mahusin
Manager for Digital Innovation and Sustainable Economy at ERIA

Hilmy Prilliadi
Reseach Associate at ERIA

[1] There is no globally accepted definition of spam (Palfrey, Abrams, Bambauer, 2005). The Regional Comprehensive Economic Partnership defined unsolicited commercial electronic messages as commercial or marketing messages sent without the recipient's consent or despite their rejection. This definition applies to unsolicited messages delivered through SMS, email, and other modes (ASEAN Secretariat et al., 2020). Spam can also be transmitted via phone calls, instant messaging, social media, and other digital channels (Mrisho, Sam, Ndibwile, 2021).

[2] Statista, Global Spam Volume as Percentage of Total E-mail Traffic from 2011 to 2023, https://www.statista.com/statistics/420400/spam-email-traffic-share-annual/ [accessed 7 September 2024]

Figure 1: Key Aspects in Combating Spam



ISP = internet service provider.
Sources: Jimmy (2024), Teixeira da Silva, Al-Khatib, Tsigaris (2020).

In ASEAN, the ASEAN Digital Masterplan 2025 advocates for regulations in ASEAN Member States (AMS) to combat spam and to protect consumers' personal information (ASEAN, 2021a). The ASEAN Committee on Consumer Protection leads regional efforts outlined under the Work Plan on the Implementation of the ASEAN Agreement on Electronic Commerce on capacity building to address online scams and to conduct training on online consumer law investigations (ASEAN, 2021b). ASEAN+1 free trade agreements, such as the upgraded ASEAN–Australia–New Zealand Free Trade Area (AANZFTA) and the Regional Comprehensive Economic Partnership (RCEP) agreement go beyond ASEAN internal cooperation, with hard regulatory commitments mandating that parties adopt and maintain measures to manage spam, enable recipients to opt out of such messages, develop consent requirements, and ensure recourse for non-compliance, while also encouraging cooperation on related regulations (ASEAN Secretariat et al., 2020; ASEAN Secretariat, Government of Australia, Government of New Zealand, 2023). The 2023 ASEAN–China Initiative on Enhancing Cooperation on E-commerce also includes combating spam as one of its key focus areas for joint capacity building (ASEAN, 2023). Moreover, the 4th ASEAN Digital Ministers Meeting welcomed the establishment of the ASEAN Working Group on Anti-online Scam as a platform for AMS to cooperate on capacity building, training, and information sharing related to combating scams, which may include spam of malicious intent (ASEAN, 2024).

Combating spam poses challenges in technical, economic, consumer protection, and regulatory domains for many countries. Technically, spam strains internet infrastructure, consumes network resources, and increases costs for both ISPs and users, particularly in countries with limited internet access and bandwidth. It also exposes users to malware and scam risks, leading to further expenses for system repairs and data theft (Internet Society, 2015). As spam evolves with new applications and data exchange methods, spammers are launching increasingly sophisticated attacks that steal personal data, damage networks, and infect systems. In response, organisations and researchers are continuously developing spam-filtering techniques to counter these threats, emphasising the need for adaptive and robust measures (Jáñez-Martino et al., 2023).

Economically, sending spam disproportionately incurs minimal costs for the spammers themselves, while the recipients, ISPs, infected users, and network operators bear the financial burden of scams or specific anti-spam software. This economic disparity perpetuates the problem as spammers continue to exploit low-cost opportunities to distribute their messages (Anderson et al., 2019).

In many AMS, consumers are not sufficiently empowered to protect themselves from online sellers and platforms. The 2020 ASEAN Consumer Empowerment Index revealed only moderate levels of consumer empowerment across ASEAN. To address this, outreach campaigns and research should target issues such as online scams, fake reviews, fraudulent shops, and counterfeit products, which pose significant enforcement challenges, especially in traceability. Enhancing consumer awareness is crucial for better protection across AMS (ASEAN, 2020).

From a regulatory perspective, enforcing spam laws is challenging due to the cross-border nature of spam, which often originates from outside of local jurisdictions. While long-arm provisions can help deter foreign spammers, effective enforcement typically requires bilateral or multilateral treaties. Without such cross-border cooperation, robust spam laws may only shift spammers to other countries rather than stop their activities (Aranda Serna, 2022). In ASEAN, while three AMS have enacted specific anti-spam legislation, the remaining AMS only incorporate spam-related provisions into existing laws. Under the RCEP and the upgraded AANZFTA, some AMS are not immediately required to implement spam-related measures, allowing them transition periods to fully comply with the agreement's requirements (ASEAN Secretariat et al., 2020; ASEAN Secretariat, Government of Australia, Government of New Zealand, 2023).

Domestic spam laws throughout ASEAN also differ in their approach, particularly between opt-in and opt-out models. The opt-in model requires prior consent or a transaction with the recipient before sending commercial electronic communications, whereas the opt-out model permits the sending of commercial emails until the recipient requests a cessation. Consequently, while ISPs may filter bulk commercial emails as spam, these emails are not always illegal.

South Korea and the United States follow an opt-out regime, while Australia, the European Union, New Zealand, Singapore, and the United Kingdom have implemented an opt-in approach (Palfrey, Abrams, Bambauer, 2005). Consequently, different approaches to spam regulation across countries and regions can complicate cross-border enforcement (Aranda Serna, 2022). For instance, as Singapore prohibits unsolicited emails while South Korea allows them until the recipient opts out, it difficult for Singapore to enforce its laws against South Korea-based spammers, highlighting the need for international coordination to enhance the effectiveness and consistency of spam legislation. To develop a consistent and effective regional anti-spam framework, a harmonised opt-in approach can reduce inconsistencies in enforcement across borders.

International collaboration on anti-spam efforts further supports the need for a unified approach. The OECD Anti-Spam Toolkit of Recommended Policies and Measures offers a regulatory handbook, self-regulatory examples, technical and user-focused protection methods, and an inventory of partnerships (OECD, 2006). Moreover, the Asia-Pacific Economic Cooperation (APEC) Principles for Action against Spam includes a voluntary programme of action and a set of principles to ensure some consistency in government approaches (APEC, 2005). The Unsolicited Communications Enforcement Network (UCENet) is a global network to combat spam through enforcement, intelligence sharing, compliance coordination, and training. UCENet is open to government and private sector representatives (UCENET, 2016).

Policy Recommendations

The diverse approaches to spam regulation, coupled with the existing hurdles, highlight the need for a more coordinated and harmonised regional framework. The following policy recommendations are proposed to enhance the effectiveness of anti-spam measures in ASEAN:

- Adopt a harmonised approach for the Digital Economy Framework Agreement (DEFA), taking into account the commitments in the RCEP and upgraded AANZFTA, including opt-in requirements for consumer protection to improve cross-border enforcement, reduce inconsistencies, and make it easier to combat spam at the regional level. Facilitate clear opt-out mechanisms to reduce spam.
- Prioritise adopting anti-spam rules and measures in parallel to the DEFA negotiations to ensure timely compliance. To effectively address the technical and legal challenges of spam enforcement across borders, AMS should also foster cooperation with external partners, drawing from the cooperative clauses in the RCEP and Comprehensive and Progressive Agreement for Trans-Pacific Partnership for sharing best practices, joint enforcement, and capacity building.
- Adopt a unified anti-spam guideline across ASEAN to simplify enforcement and to inspire improvements in countries with weak legislation. Strengthening legislation with stronger penalties for non-compliance to make it more difficult for spammers to exploit weak regulations and increase pressure on countries that permit spam.
- Launch targeted outreach and capacity-building initiatives to raise consumer and business awareness of the risks associated with spam, including educating them on how to identify and to report spam.
- Encourage investment in advanced spam-filtering and machine-learning solutions to address spam threats. AMS can incentivise ISPs and tech companies to develop and to deploy innovative anti-spam technologies.

References

Alazab, M. and R. Broadhurst (2015), 'Spam and Criminal Activity', *Trends and Issues in Crime and Criminal Justice (Australian Institute of Criminology)*, 52, https://ssrn.com/abstract=2467423 or http://dx.doi.org/10.2139/ssrn.2467423

Anderson, R. et al. (2019), 'Measuring the Changing Cost of Cybercrime', 18th Annual Workshop on the Economics of Information Security, Boston, 3–4 June,

Aranda Serna, F.J. (2022), 'The Legal Regulation of Spam: An International Comparative Study', *Journal of Innovations in Digital Marketing*, 3(1), pp.1–11, https://doi.org/10.51300/jidm-2022-44

Asia-Pacific Economic Cooperation (APEC) (2005), *APEC Principles for Action against Spam*, APEC Telecommunications and Information Ministerial Meeting, Lima, 1–3 June.

Association of Southeast Asian Nations (ASEAN) (2020), *The Report of ASEAN Consumer Empowerment Index 2020 Pilot Project*, Jakarta.

––––– (2021a), *ASEAN Digital Masterplan 2025*, Jakarta.

––––– (2021b), *Work Plan on the Implementation of ASEAN Agreement on Electronic Commerce*, Jakarta.

––––– (2023), 'ASEAN-China Initiative on Enhancing Cooperation on E-commerce', 22nd AEM-MOFCOM Consultation, Semarang, Indonesia, 21 August.

––––– (2024), 'The 4th ASEAN Digital Ministers' Meeting and Related Meetings Joint Media Statement', 2 February.

ASEAN Secretariat, *Government of Australia, and Government of New Zealand (2023), Second Protocol to Amend the Agreement Establishing the ASEAN-Australia-New Zealand Free Trade Area*.

ASEAN Secretariat et al. (2020). *Regional Comprehensive Economic Partnership Agreement*.

Australian Institute of Criminology (2010), 'More Malware – Adware, Spyware, Spam and Spim', *High-tech Crime Briefs*, No. 11, Canberra.

Internet Governance Forum (2024), 'Regulation and Mitigation of Unwanted Communications', draft.

Internet Society (2015), 'The Challenge of Spam: An Internet Society Public Policy Briefing', 30 October.

INTERPOL (2020), *ASEAN Cyberthreat Assessment 2020: Key Insights from the ASEAN Cybercrime Operations Desk*, Singapore.

Jáñez-Martino, F., et al. (2023), 'A Review of Spam Email Detection: Analysis of Spammer Strategies and the Dataset Shift Problem', Artificial Intelligence Review, 56(2), pp.1145–73, https://doi.org/10.1007/s10462-022-10195-4

Jimmy, F. (2024), 'Cybersecurity Vulnerabilities and Remediation through Cloud Security Tools', Journal of Artificial Intelligence General Science, 3(1).

Karim, A. et al. (2019), 'A Comprehensive Survey for Intelligent Spam Email Detection', IEEE Access, https://doi.org/10.1109/ACCESS.2019.2954791

Mrisho, Z.K., A.E. Sam, and J.D. Ndibwile (2021), 'Low Time Complexity Model for Email Spam Detection Using Logistic Regression', *International Journal of Advanced Computer Science and Applications*, 12(12), pp.112–18.

Organisation for Economic Co-operation and Development (OECD) (2006), *OECD Anti-Spam Toolkit of Recommended Policies and Measures*, Paris.

Palfrey, J., D. Abrams, and D.E. Bambauer (2005), *A Comparative Analysis of Spam Laws: The Quest for a Model Law*.

Statista, Global Spam Volume as Percentage of Total E-mail Traffic from 2011 to 2023, https://www.statista.com/statistics/420400/spam-email-traffic-share-annual/ [accessed 7 September 2024]

Teixeira da Silva, J.A., A. Al-Khatib, and P. Tsigaris (2020), 'Spam Emails in Academia: Issues and Costs', *Scientometrics*, 122(2), pp.1171–88, https://doi.org/10.1007/s11192-019-03315-5

Unsolicited Communications Enforcement Network (UCENET), Who We Are, https://www.ucenet.org/who-we-are/

ERIA

Sentral Senayan II, 5th, 6th, 15th floors
Jalan Asia Afrika No. 8
Senayan, Central Jakarta 10270, Indonesia
Tel: (62-21) 57974460 Fax: (62-21) 57974463
E-mail: contactus@eria.org