IPS Working Papers

BORROWING BERLO: ENHANCING PUBLIC UNDERSTANDING OF SINGAPORE'S ONLINE HARMS LAWS THROUGH THE SMCR MODEL OF COMMUNICATION

CHEW HAN EI
CAROL SOON
and
NATALIE CHIA

July 2025
IPS Working Papers No. 63

Institute of Policy Studies

About Institute of Policy Studies (IPS)

The Institute of Policy Studies (IPS) was established in 1988 to promote a greater awareness of policy issues and good governance. Today, IPS is a think-tank within the Lee Kuan Yew School of Public Policy (LKYSPP) at the National University of Singapore. It seeks to cultivate clarity of thought, forward thinking and a big-picture perspective on issues of critical national interest through strategic deliberation and research. It adopts a multi-disciplinary approach in its analysis and takes the long-term view. It studies the attitudes and aspirations of Singaporeans which have an impact on policy development and the relevant areas of diplomacy and international affairs. The Institute bridges and engages the diverse stakeholders through its conferences and seminars, closed-door discussions, publications, and surveys on public perceptions of policy.

IPS Working Papers No. 63

BORROWING BERLO: ENHANCING PUBLIC UNDERSTANDING OF SINGAPORE'S ONLINE HARMS LAWS THROUGH THE SMCR MODEL OF COMMUNICATION

Chew Han Ei
Senior Research Fellow
Head, Governance & Economy
Institute of Policy Studies
National University of Singapore
han.chew@nus.edu.sg

Carol Soon
Associate Professor (Practice)
Department of Communications and New Media
National University of Singapore
carol.soon@nus.edu.sg

and

Natalie Chia
Director of Research
SG Her Empowerment (SHE)
natalie.chia@she.org.sg

July 2025

CONTENTS

BORROWING BERLO:
ENHANCING PUBLIC UNDERSTANDING OF SINGAPORE’S ONLINE HARMS LAWS THROUGH THE SMCR MODEL OF COMMUNICATION

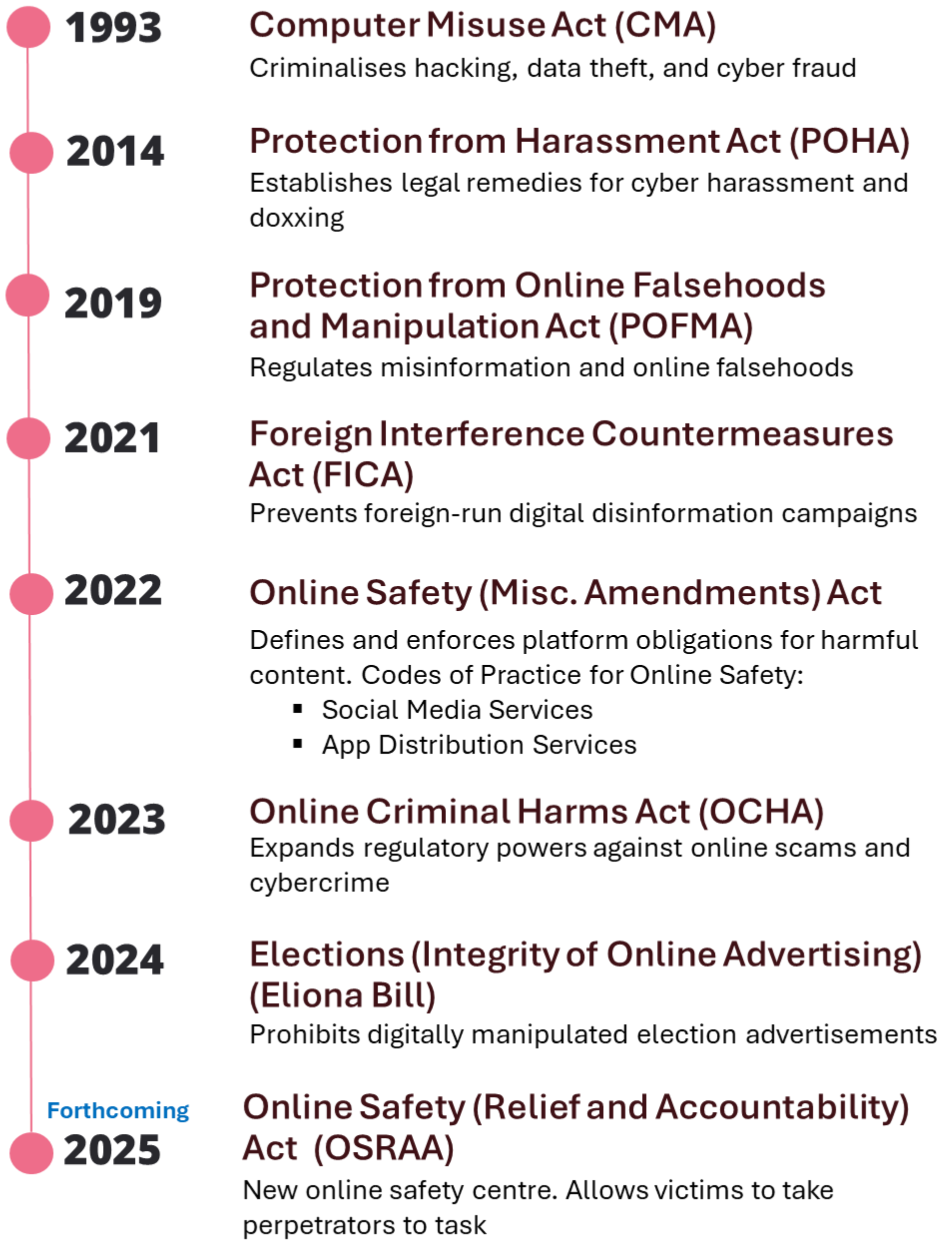
1. INTRODUCTION

Singapore’s approach to online harms is both ambitious and multifaceted. From misinformation and digital abuse to election interference and foreign influence, a growing body of legislation has emerged over the past decade to regulate behaviour and protect citizens in the digital domain. These laws are comprehensive and arguably world-leading; but for the average citizen, policymaker or media professional, they can feel like an alphabet soup, e.g., POHA, POFMA, OCHA, FICA, CMA, ELIONA, and soon, OSRAA (see Figure 1).[1]

Legislation plays important roles, such as providing the authorities with the necessary levers to act against offences and perpetrators and giving victims legal recourse to seek justice and compensation for the harms they suffer.

[1] The Criminal Law Reform Act (CLRA) in 2019 was a comprehensive piece of legislation that significantly updated the Penal Code and other related acts. This reform also criminalised cyber-flashing (sending nudes), voyeurism and doxxing. The Online Safety (Miscellaneous Amendments) Act 2022 is an Act to amend the *Broadcasting Act 1994* and the Electronic Transactions Act 2010 to regulate providers of online communication services.

Figure 1: Key legislation against online harms in Singapore in chronological order



1993 — **Computer Misuse Act (CMA)**
Criminalises hacking, data theft, and cyber fraud

2014 — **Protection from Harassment Act (POHA)**
Establishes legal remedies for cyber harassment and doxxing

2019 — **Protection from Online Falsehoods and Manipulation Act (POFMA)**
Regulates misinformation and online falsehoods

2021 — **Foreign Interference Countermeasures Act (FICA)**
Prevents foreign-run digital disinformation campaigns

2022 — **Online Safety (Misc. Amendments) Act**
Defines and enforces platform obligations for harmful content. Codes of Practice for Online Safety:

- Social Media Services
- App Distribution Services

2023 — **Online Criminal Harms Act (OCHA)**
Expands regulatory powers against online scams and cybercrime

2024 — **Elections (Integrity of Online Advertising) (Eliona Bill)**
Prohibits digitally manipulated election advertisements

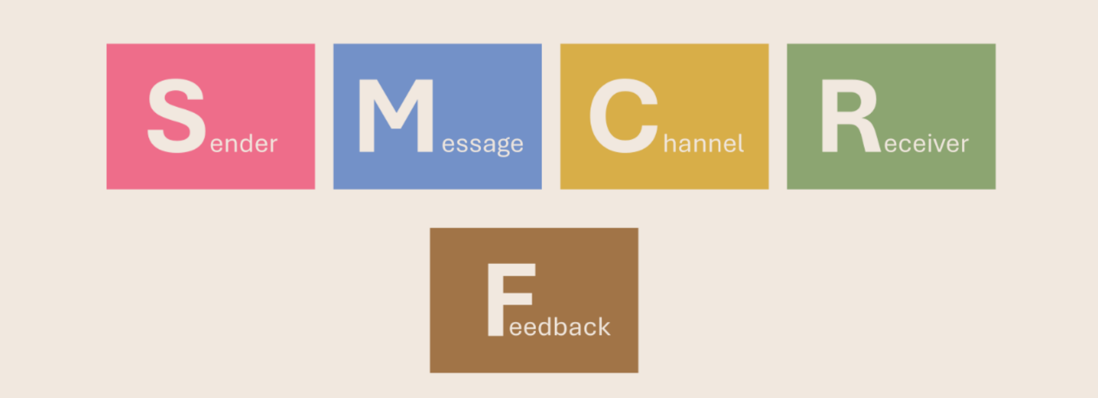
Forthcoming **2025** — **Online Safety (Relief and Accountability) Act (OSRAA)**
New online safety centre. Allows victims to take perpetrators to task

However, a forthcoming study by the three authors of this working paper and a study by the second author (Soon, Goh & Bala Krishnan, 2023) point to confusion and low awareness among Singapore residents about the legal protections available to them, due in part to the complexity of the existing legislative landscape. Low public understanding and confusion also hinder individuals from seeking redress effectively. A study by SG Her Empowerment (SHE, 2025) found that some individuals experiencing online harms hesitated to seek help from authorities, uncertain whether their experiences met the threshold for legal or other official intervention.

2. BORROWING BERLO

This working paper provides an organising framework to help citizens and stakeholders involved in education and support services navigate the landscape more effectively. Drawing on David K. Berlo's classic SMCR model of communication (1960), this working paper proposes a way to classify these laws not by chronology or legal domain, but by the communicative functions and points of intervention they target. The SMCR model is introduced here as a taxonomy grounded in the logic of a communication chain (see Figure 2). While Berlo originally conceived of it as a dynamic model of communication flow — from sender to receiver — our application repurposes its distinct components to map legal interventions according to where they aim to disrupt harm along the communication chain.

Figure 2: Classic SMCR model of communication (plus feedback)



Think of it as a map of functions for understanding online harms:

- Sender: Who is doing harm?
- Message: What content is harmful?
- Channel: Through which services or platforms is harm transmitted?
- Receiver: Who is harmed, and how are they protected?

- Feedback: How do regulators monitor compliance and course-correct?

While this structure helps to organise legal responses by communicative functions, it does not imply that each law operates in just one domain. Many laws address multiple parts of the communication chain at once. We return to this point after the taxonomy.

2.1. Sender: Laws Targeting Perpetrators

Every harmful online act originates from a source — the person who initiates the behaviour or the publisher responsible for producing the content in question. In the SMCR framework, this is the “sender”. Effective regulation must therefore include robust mechanisms to deter, investigate and hold individuals or groups who commit online harms accountable. Targeting the sender helps prevent escalation, deters would-be offenders and reaffirms social norms about acceptable behaviour online.

Singapore’s legislation provides for a range of enforcement and regulatory levers aimed squarely at perpetrators. These include criminal penalties such as fines and imprisonment for serious cyber offences, the issuance of Protection Orders to restrain perpetrators from committing further harassment, and account restrictions.

Illustrative laws and enforcement examples:

- Protection from Harassment Act 2014: Criminalises online harassment, stalking, doxxing and related forms of personal abuse. Provides for protection orders and compensation. *Example: In late 2023 and early 2024, a 34-year-old former NTU researcher repeatedly stalked a PhD student—sending him 116 emails, visiting his workplaces despite a court-issued protection order—and was subsequently fined S$8,000 after pleading guilty under the Protection from Harassment Act.*

- Computer Misuse Act 1993: Addresses unauthorised access to data, system intrusion and use of malware. *Example: In 2025, a former employee of the National Dental Centre Singapore was handed two charges under the Computer Misuse Act for accessing the personal details of patients in addition to charges of taking voyeuristic images of female patients.*

Online Criminal Harms Act 2023: Tackles evolving criminal harms online and makes special provisions for scams and malicious cyber activities. *Under OCHA, a Stop Communication direction requires the recipient, who can be an individual or an entity, to stop communicating the specified online content to people in Singapore. No specific number of cases publicly reported to date, though the law has been cited in enforcement operations targeting child sexual exploitation material (CSEA) and online drug trafficking.*

2.2. Message: Regulating Harmful Content

The second component of the model concerns the “message” — the content shared or transmitted online. Regulating harmful content is essential for reducing misinformation, protecting vulnerable communities and preserving the integrity of public discourse. These laws deal with *what* is being said, rather than *who* is saying it.

Message-focused legislation serves two key functions: first, to define what constitutes harmful content; and second, to enable corrective or enforcement actions after such content has caused or risks causing harm. In Singapore, these laws empower authorities to issue content removal orders and takedown notices, especially for egregious material like self-harm content or child sexual exploitation. Misinformation is countered through correction notices, and digital platforms are required to deploy enhanced AI moderation as well as human oversight to assess flagged content. Social media companies are also held accountable for the circulation of false or manipulated political messages, particularly in the lead-up to elections.

Illustrative laws and enforcement examples:

- Protection from Online Falsehoods and Manipulation Act 2019: Defines what constitutes a falsehood and mandates correction of false or misleading content that harms public interest. *Example: During the pandemic, POFMA warnings were issued to correct false statements about COVID-19 vaccine side effects.*

- Online Safety (Miscellaneous Amendments) Act 2022: Enables the issuance of directions to disable access by Singapore users based on defined forms of egregious content, such as content advocating or instructing on suicide or self-harm, physical or sexual violence and terrorism; content depicting child sexual exploitation; content posing public health risks in Singapore; and content likely to cause racial and religious disharmony in Singapore. *The 2024 IMDA Online Safety Assessment Report lists actions taken by the six designated social media services, including content takedowns and account removals.*

- Elections (Integrity of Online Advertising) Act 2024: Bans the publication of false digital depictions of candidates, including deepfakes, during election periods to uphold the integrity of Singapore's elections. *No case cited yet.*

2.3. Channel: Managing Platforms and Services

Communication is enabled through channels and in today's digital environment, those channels are social media services and online service providers. Managing the channel means ensuring these intermediaries are safe, transparent and cooperative. These laws define platforms' (or channels') obligations and prescribe what they must do to monitor, block and report harmful behaviour. Singapore's regulatory approach to platforms includes several enforcement levers. Authorities may issue service restriction or access blocking orders for non-compliant platforms, compelling them to suspend harmful services. Platforms found failing to meet moderation obligations may be held legally liable.

Illustrative laws and enforcement examples:

- Online Safety (Miscellaneous Amendments) Act 2022: Defines regulated online communication services subject to amendments to Broadcasting Act 1994 and Electronic Transactions 2010. Based on categories of egregious content, IMDA can issue directives to disable access to such content or block services that fail to comply. *Example: In October 2021 (prior to the enactment of the Act), IMDA suspended the class license of The Online Citizen to run its website for repeatedly failing to declare all sources of funding.*

- Foreign Interference (Countermeasures) Act 2021: Also known as FICA, this allows the government to issue directions to various entities, including social media services and website operators, to take down or block content, disclose information about foreign actors, and designate "politically significant persons" who may be subject to specific requirements. *Example: Singapore invoked FICA on 19 July 2024 to require five social media platforms to block 95 accounts that published coordinated posts, making them inaccessible to Singapore-based users.*

- Online Criminal Harms Act 2023: Empowers government agencies to issue directions to online service providers, internet service providers and app stores to restrict access to criminal content and limit further exposure to criminal activities on non-compliant online services.

- Elections (Integrity of Online Advertising) Act 2024: Imposes financial penalties on non-compliant platforms. *No case cited yet.*

2.4. Receiver: Protecting Victims and Users

Victims are the most direct recipients of harm in the communication process. In some cases, victims could be the public in general who are susceptible to harmful content; for example, false statements of facts that threaten public health or Singapore's security. The "receiver" component acknowledges their centrality and the need for clear, accessible protections. Such protections are complemented by wider systemic support.

Remedial measures include avenues for compensation in cases of online abuse, alongside access to legal and psychological support services provided by community organisations. Victim-reporting mechanisms are being strengthened on major platforms. These collective efforts ensure that those harmed online are not left to navigate the aftermath alone.

Illustrative laws and enforcement examples:

- Protection from Harassment Act 2014: Enables Protection Orders and civil claims for damages. In 2024, the number of protection order applications to Singapore's Protection from Harassment Court reached 631, up from 526 in 2023, 520 in 2022 and 346 in 2021.

- Code of Practice for Online Safety (IMDA, 2023): Aims to enhance online safety, particularly for children, and curb the spread of harmful content on social media platforms. Designated social media services are required to implement measures to minimise users' exposure to harmful content, provide users with reporting tools, and be transparent about their safety measures.

2.4.1. What's next in protecting users: OSRAA (forthcoming)

The forthcoming Online Safety (Relief and Accountability) Act (OSRAA) will further expand Singapore's regulatory toolkit. Announced by Prime Minister Lawrence Wong in 2024 at the launch of Smart Nation 2.0, OSRAA aims to provide stronger assurance to victims and raise accountability standards.

Proposed measures include:

- A new Online Safety Centre to receive victims' complaints and act on them swiftly.
- New statutory torts for civil claims against perpetrators.
- Enhanced user information disclosure to aid investigations.

2.5. Feedback: Regulatory Oversight and Compliance

No system of regulation is complete without oversight. In the context of online harms, feedback mechanisms ensure that laws translate into action and that platforms are held accountable for how they respond to harmful content.

Several laws mandate transparency and reporting. Under POFMA and the Online Safety (Miscellaneous Amendments) Act, platforms must regularly publish reports detailing takedown actions, categories of flagged content and the measures taken to reduce exposure to harm. These requirements increase visibility into platform practices and support public scrutiny.

These measures collectively help ensure that online safety regulations remain responsive, enforceable and grounded in real-world outcomes.

Illustrative laws:

- Online Safety (Miscellaneous Amendments) Act 2022: Under the Code of Practice for Online Safety in Singapore, designated social media services, like Facebook, Instagram and TikTok, must minimise users' exposure to harmful content, empower users with reporting tools and **submit annual transparency reports to IMDA.** These reports detail the platforms’ measures to tackle harmful content and their effectiveness in maintaining online safety (see 2024 Online Safety Assessment Report).

- Protection from Online Falsehoods and Manipulation Act 2019: Under one of the Codes of Practice, prescribed internet intermediaries must provide the POFMA Office with an annual report on the implementation of measures to prevent and counter the abuse of online accounts.

3. WHY WE ORGANISE LAWS THIS WAY?

Applying the SMCR model to Singapore’s online harms laws is not merely an academic exercise; it is a pragmatic response to a real-world challenge. By organising laws according to communication functions rather than chronology or statute origin, the model helps clarify what is often perceived as a complex and patchworked space.

The model allows us to move beyond acronyms and enforcement headlines to surface what the laws are functionally designed to do. Is it targeting the source of harm? The message itself? The channel transmitting the harm? Protecting the person on the receiving end? Or the system for oversight and accountability?

The model does not suggest that each law operates within a single domain of harm (e.g., targeting only the sender or the channel). In reality, many laws contain provisions that span across multiple functions — enabling authorities to act on the sender, the message and the channel, while also protecting the receivers and providing them with means of seeking recourse. For example, POFMA empowers authorities to require both the sender (e.g., content creator) and the channel (e.g., a social media service) to publish corrections and stop the communication of a false content (i.e., a false statement of fact). The receiver (the Minister in this case) has the right to direct IMDA to issue the necessary direction.

Organising laws functionally has several purposes. First, it makes the policy intent of each law clearer, allowing even non-specialists to understand the rationale for specific interventions. Second, it supports public education by translating legal provisions into intuitive categories. Third, it creates shared vocabulary for policymakers, regulators, platform providers and civil society to align efforts and clarify accountability.

Rather than situating each law within its own legislative history, the SMCR framework reveals how they work *together* as a system. This systemic view enables collective public discourse on legislative gaps and how our legal architecture might evolve to meet emerging forms of harm.

4. IMPLICATIONS FOR PUBLIC COMMUNICATION

The SMCR framework is not meant to be applied “as-is” in public-facing communications. Rather, it offers a useful heuristic for policymakers and communications teams to clarify what each law is targeting and where the public may need better guidance.

Consider, for instance, the hesitation some individuals face when deciding whether to report online harms. The issue is not simply a lack of awareness. Often, it stems from uncertainty about whether their experiences meets a legal threshold, or what avenues for redress exist. The SMCR model helps pinpoints these friction points — mapping, in this case, to the “message” (the harmful content) and “receiver” (available remedies).

As a planning tool, this structure can support more intentional messaging across different agencies. However, it needs to be translated for public audiences, anchored in concrete examples, conveyed in plain language and paired with clear calls to action.

5. CONCLUSION

Singapore has built one of Asia's most robust legal ecosystems for addressing online harms. But legal robustness is not the same as public understanding. For laws to be effective, people must be able to navigate them — not just as legal texts, but as part of a larger social contract about digital safety and responsibility.

This working paper proposes a simple organising model that classifies online harms laws by what they address:

- The source of the harm (perpetrator)
- The harmful content itself
- The platforms that transmit it
- The individuals harmed
- And the mechanisms for oversight and redress

Borrowing from Berlo's SMCR model, we offer a simple but structured way to map the regulatory landscape. The goal is not to flatten complexity into a simplistic model, but to provide an intuitive framework for understanding how these laws function together. It is a tool for public education, cross-agency coordination and future-proof policymaking. Social service agencies such as SG Her Empowerment can adopt and adapt this framework in their own public education and engagement efforts.

Above all, this working paper is a call to make our digital safety infrastructure not just legally sound, but communicatively clear. Because in the end, while efforts matter, so does how we understand them.

5.1. Authors' Note

This working paper will be updated following the enactment of the forthcoming Online Safety (Relief and Accountability) Act (OSRAA), to reflect the new legal provisions, enforcement mechanisms and institutional arrangements introduced. As OSRAA represents a significant shift toward civil remedies and victim support in Singapore's regulatory landscape, its inclusion will be essential to keeping this taxonomy current and analytically robust.

5.2. Acknowledgements

We thank Dr Michele Khoo for her generous and sharp review of an early draft. Her insights helped clarify that while the SMCR model works well as a framing device, its real value for public communication lies in how it supports strategy.

REFERENCES

Berlo, D. K. (1960). *The Process of Communication: An Introduction to Theory and Practice*. New York: Holt, Rinehart and Winston.

SG Her Empowerment (SHE). (2025). *404 Help Not Found: Lived experiences of online harms survivors*. SHE. https://she.org.sg/news/404-help-not-found-lived-experiences-of-online-harms-survivors

Shannon, C. E., & Weaver, W. (1949). *The Mathematical Theory of Communication,* pp.1–7. University of Illinois Press.

Singapore Statutes Online. Retrieved from https://sso.agc.gov.sg:

- Computer Misuse Act 1993
- Protection from Harassment Act 2014
- Protection from Online Falsehoods and Manipulation Act 2019
- Foreign Interference (Countermeasures) Act 2021
- Online Safety (Miscellaneous Amendments) Act 2022
- Online Criminal Harms Act 2023
- Elections (Integrity of Online Advertising) Act 2024

Soon, C., Goh, S. & Bala Krishnan, N. (2023, January). Study on Singaporeans and False Information Phase Two and Phase Three — Immunity and Intervention. *IPS Exchange Series No. 23*. Institute of Policy Studies.

APPENDIX 1: ABOUT THE AUTHORS

CHEW Han Ei leads the Governance & Economy cluster at the Institute of Policy Studies (IPS). His work focuses on quantitative policy research, with a strong interest in online harms, digital trust and technology adoption.

He has served as Principal Investigator for multiple large-scale research grants and collaborates closely with public agencies to inform decision-making and policy development. His approach is empirically grounded and hands-on — from designing social science research projects to leading data analyses that shape real-world outcomes.

Outside of IPS, Han Ei serves on the board of SG Her Empowerment and is a pro bono Research Consultant to UNESCO. Some of his key international projects for UNESCO include Reading in the Mobile Era and I'd Blush If I Could – Closing Gender Divides in Digital Skills through Education.

Han Ei earned his PhD in Media and Information Studies from Michigan State University, USA. He also writes *The Chart Doctor Has Issues* — a Substack newsletter on data storytelling, visual best practices and the occasional chart takedown.

Carol **SOON** is Associate Professor (Practice) at the Department of Communications and New Media in the National University of Singapore (NUS). She is a member of the World Economic Forum's Global Future Council on

Information Integrity (2025 to 2026) and Principal Investigator at the NUS Centre for Trusted Internet and Community. She is also Adjunct Principal Scientist at the Centre for Advanced Technologies in Online Safety (CATOS) that is set up by the Ministry of Digital Development and Information.

Her research interests are in media regulation and digital policy, social media governance, digital literacy and policy communication. Dr Soon has written about 50 media commentaries on the impact of technology, media regulation, digital literacy and digital upskilling of citizens and workers, and public communication. She has single-authored and co-authored more than 80 research reports, journal articles, book chapters and conference papers. To share research findings with diverse stakeholders, she has spoken at and chaired over 90 talks on a variety of international and local platforms.

Dr Soon is currently Vice Chair of Singapore's Media Literacy Council. She is also a member of the Ministry of Culture, Community and Youth's Co-Governance Community of Practice, and serves on the National Crime Prevention Council.

Natalie **CHIA** is Director of Research at SG Her Empowerment (SHE), an independent non-profit supporting girls and women in the online and offline space. In its online harms workstream, SHE has examined online harms' prevalence and impact on individuals and society. It has investigated online harms' long-term effects on survivors, patterns of help-seeking behaviour, and ecosystem-based approaches to strengthening digital safety. SHE's work has also focused on specific population segments, such as youth — investigating concerns around algorithmic recommendations and cancel culture. Looking ahead, SHE is deepening its research into emerging harms linked to generative AI, with particular attention to gender norms as underlying mechanisms shaping these new forms of risk.

SHE is concerned with the normalisation of online harms in society — especially as it relates to harmful conduct directed at girls and women — and how this shapes discourse in Singapore's online spaces. SHE's research insights inform the SHECARES@SCWO support centre for victims of online harms, as well as public education and advocacy efforts towards a safer and more equitable digital society for all.

Natalie holds a master's from the Oxford Department of International Development, completed in 2019. Prior to joining SHE, she held research roles across government, academia and the non-profit sector — including at the Ministry of Communications and Information (since renamed), the National Council of Social Service, the Institute of Policy Studies and UNICEF.

About IPS Working Paper Series

The IPS Working Papers Series is published in-house for early dissemination of works-in-progress. This may be research carried out by IPS researchers, work commissioned by the Institute or work submitted to the Institute for publication.

The views expressed in the Working Papers are strictly those of the author(s) alone and do not necessarily reflect the views of the IPS.

Comments on the Working Papers are invited. Please direct your comments and queries to the author(s).

IPS Working Papers are available from the IPS at $7.00 each (before GST). Postage and handling charges will be added for mail orders.

For more information, please visit www.lkyspp.nus.edu.sg/ips or
contact email: ips@nus.edu.sg.

Institute of Policy Studies
Lee Kuan Yew School of Public
Policy National University of
Singapore
1C Cluny Road House 5
Singapore 259599

Web: www.lkyspp.nus.edu.sg/ips
Registration Number: 200604346E