Published on 8 April 2025

MEDIATING ONLINE CRIMINAL HARMS THROUGH THE LAW[1]

[2025] SAL Prac 9

In recent times, there have been grave concerns about how online content may be harmful to individuals and the public. Of particular concern is how harmful content online can impact the well-being of individuals negatively, especially in the case of younger and more vulnerable persons, which may result in self-harm or even death. This article will attempt to mediate the balance between managing online criminal harms and the rights of the individual by looking at the legislative framework, the concerns at hand and what can be done to address them in this age of technology.

Melvin **LOH**
LLB (National University of Singapore),
LLM (Judicial Studies) (Singapore Management University);
Advocate and Solicitor (Singapore);
Senior Lecturer, School of Law, Singapore University of Social Sciences;
Counsel, Peter Low Chambers LLC.

I. Introduction

1 As of February 2025, there were 5.56 billion Internet users worldwide, which amounted to 67.9% of the global population.[2] Out of this number, 5.24 billion, or 63.9% of the world's population, were social media users.[3] Upon this backdrop, there have been serious concerns internationally about the need to

1 An earlier version of this paper was presented at the International Conference on Regulating Technology in Asia (7–8 March 2024).

2 Ani Petrosyan, Number of internet and social media users worldwide as of February 2025", *Statistics* (13 February 2025) <https://www.statista.com/statistics/617136/digital-population-worldwide/> (accessed 25 March 2025).

3 Ani Petrosyan, Number of internet and social media users worldwide as of February 2025", *Statistics* (13 February 2025) <https://www.statista.com/statistics/617136/digital-population-worldwide/> (accessed 25 March 2025).

develop suitable safeguards, legal and otherwise, to help combat the potential harms that come with online Internet usage. This article seeks to examine how Singapore has tried to address some of these concerns by implementing legislative changes and how such laws, including the Online Safety (Miscellaneous Amendments) Act 2022[4] ("OSMAA") and the Online Criminal Harms Act 2023[5] ("OCHA") mediate the balance of public policy and the use of the online space. The analysis explores the current legal landscape in Singapore and recent developments before considering what else can done in regulating the online space.

II. Online safety and harm

A. Online Safety (Miscellaneous Amendments) Act 2022

(1) Dealing with harmful online content

2 In January 2022, a survey by the Sunlight Alliance for Action found that almost half of the respondents had personally encountered harmful online content.[6] Another survey in June 2022 by the Ministry of Communications and Information found that respondents were most concerned with harms affecting children, with a high majority (97%) who felt that harmful online content can have at least moderate impact on children and youths.[7] Ultimately, survey results revealed that sexual content,

4 Act 38 of 2022.
5 Act 24 of 2023.
6 An online poll conducted by Sunlight Alliance for Action ("Sunlight AfA") in January 2022, with more than 1,000 Singaporeans on their perceptions, experiences, and the prevalence of online harms in Singapore. The Sunlight AfA was launched in July 2021 to tackle online harms, especially those targeted at women and girls. The Sunlight AfA takes a whole-of-nation partnership approach and members of the Sunlight AfA include individuals across the 3P sectors (*ie*, Public, Private, and People), coming together with the aim of closing the digital safety gap and creating an inclusive digital space: "First Reading of Online Safety (Miscellaneous Amendments) Bill", *Ministry of Digital Development and Information*, press release (3 October 2022) at para 4 <https://www.mddi.gov.sg/media-centre/press-releases/first-reading-of-online-safety-bill/> (accessed 21 March 2025).
7 "First Reading of Online Safety (Miscellaneous Amendments) Bill", *Ministry of Digital Development and Information*, press release (3 October 2022) at para 4 <https://www.mddi.gov.sg/media-centre/press-releases/first-reading-of-online-safety-bill/> (accessed 21 March 2025).

cyberbullying and violent content were the top three types of content that respondents felt the young needed to be protected from most.[8]

3 The OSMAA was passed in the Singapore Parliament on 9 November 2022 and took effect from 1 February 2023.[9] It seeks to enhance online safety for Singapore users by introducing a new part to the Broadcasting Act 1994[10] ("BA") to regulate online communication services ("OCSs") accessible by Singapore users.[11] OSMAA essentially applies to the OCSs specified in the new Fourth Schedule under the BA, which now deals with social media services ("SMSs") and app distribution services.

4 Through OSMAA, the Infocomm Media Development Authority ("IMDA"):[12]

> … can issue directions to disable access by Singapore users to egregious content found on OCSs. Egregious content includes 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.

8 "First Reading of Online Safety (Miscellaneous Amendments) Bill", *Ministry of Digital Development and Information*, press release (3 October 2022) at para 4 <https://www.mddi.gov.sg/media-centre/press-releases/first-reading-of-online-safety-bill/> (accessed 21 March 2025).

9 "Online Safety (Miscellaneous Amendments) Act Takes Effect on 1 February 2023", *Ministry of Digital Development and Information*, press release (31 January 2023) at para 1 <https://www.mddi.gov.sg/media-centre/press-releases/online-safety-act-takes-effect-on-1-february-2023/> (accessed 21 March 2025).

10 2020 Rev Ed.

11 "Online Safety (Miscellaneous Amendments) Act Takes Effect on 1 February 2023", *Ministry of Digital Development and Information*, press release (31 January 2023) <https://www.mddi.gov.sg/media-centre/press-releases/online-safety-act-takes-effect-on-1-february-2023/> (accessed 21 March 2025) at para 3; Broadcasting Act 1994 (2020 Rev Ed), Fourth Schedule.

12 "Online Safety (Miscellaneous Amendments) Act Takes Effect on 1 February 2023", *Ministry of Digital Development and Information*, press release (31 January 2023) at para 4 <https://www.mddi.gov.sg/media-centre/press-releases/online-safety-act-takes-effect-on-1-february-2023/> (accessed 21 March 2025).

(2) Directions

5 There are three types of directions that IMDA can issue:[13]

(a) A direction to an OCS provider to disable access by Singapore users to the egregious content on the service.[14] This requires the OCS provider to ensure that the specified egregious content (*eg*, a particular post) cannot be viewed by Singapore users.

(b) A direction to an OCS provider to stop the delivery or communication of content to Singapore users.[15] This can be effected by blocking the flow of content from a specified source on the OCS provider (*eg*, an account, group or channel) that is communicating the specified egregious content.

(c) A direction can be issued to an Internet access service provider to block access by Singapore users to the non-compliant OCS if the OCS provider fails to comply with IMDA's direction(s).[16]

(3) Codes of practice

6 Further, IMDA may also designate OCSs with significant reach or impact as regulated online communication services ("ROCSs").[17]

The ROCS providers will be required to comply with codes of practice which may require them to put in place systems and processes on their services to mitigate the risks of danger to Singapore users from exposure to harmful content and provide accountability to their users on such measures.

13 "Online Safety (Miscellaneous Amendments) Act Takes Effect on 1 February 2023", *Ministry of Digital Development and Information*, press release (31 January 2023) at para 5 <https://www.mddi.gov.sg/media-centre/press-releases/online-safety-act-takes-effect-on-1-february-2023/> (accessed 21 March 2025).

14 Broadcasting Act 1994 (2020 Rev Ed) s 45H(1)(*c*)(i).

15 Broadcasting Act 1994 (2020 Rev Ed) s 45H(1)(*c*)(ii).

16 Broadcasting Act 1994 (2020 Rev Ed) s 45J.

17 "Online Safety (Miscellaneous Amendments) Act Takes Effect on 1 February 2023", *Ministry of Digital Development and Information*, press release (31 January 2023) at para 6 <https://www.mddi.gov.sg/media-centre/press-releases/online-safety-act-takes-effect-on-1-february-2023/> (accessed 21 March 2025).

7 The IMDA introduced the Code of Practice for Online Safety ("Code of Practice") for designated SMSs, which came into effect on 18 July 2023. The Code of Practice mitigates the risks from harmful social media content to Singapore users, especially children, by requiring designated SMSs to enhance online safety in Singapore and curb the spread of harmful content on their services.[18] The categories of harmful content covered by the Code of Practice are: sexual content; violent content; suicide and self-harm content; cyberbullying content; content endangering public health; and content facilitating vice and organised crime.[19]

8 OSMAA empowers IMDA to designate SMSs with significant reach or impact in Singapore to comply with online codes of practice such as the Code of Practice. The designated SMSs are Facebook, HardwareZone, Instagram, TikTok, Twitter (now known as "X"), and YouTube.[20]

9 The Code of Practice was developed and refined through extensive consultation with various stakeholders, such as the public, academics and industry, to understand public concerns and operational considerations.[21] In particular, the designated SMSs were engaged extensively and were invited to submit formal responses to the Code of Practice.[22]

---

18 "IMDA's Online Safety Code Comes Into Effect", *Infocomm Media Development Authority* (17 July 2023) <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/imdas-online-safety-code-comes-into-effect> (accessed 21 March 2025).

19 "IMDA's Online Safety Code Comes Into Effect", *Infocomm Media Development Authority* (17 July 2024) <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/imdas-online-safety-code-comes-into-effect> (accessed 21 March 2025).

20 "IMDA's Online Safety Code Comes Into Effect", *Infocomm Media Development Authority* (17 July 2024) <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/imdas-online-safety-code-comes-into-effect> (accessed 21 March 2025).

21 "IMDA's Online Safety Code Comes Into Effect", *Infocomm Media Development Authority* (17 July 2024) <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/imdas-online-safety-code-comes-into-effect> (accessed 21 March 2025).

22 "IMDA's Online Safety Code Comes Into Effect", *Infocomm Media Development Authority* (17 July 2024) <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/imdas-online-safety-code-comes-into-effect> (accessed 21 March 2025).

10 Crucially, designated social media service providers must do the following under the Code of Practice:[23]

1. Minimise Singapore users' exposure to harmful content, with additional protection for children

Put in place systems and processes to tackle harmful content, including community guidelines and effective content moderation measures.

Users will be empowered with tools to manage their own safety. These may include tools to hide harmful content and unwanted interactions, limit location sharing and the visibility of their accounts from other users.

Apply age-appropriate policies to accounts belonging to children, including having a set of community guidelines appropriate for children, content moderation, and online safety information that children can easily understand. Accounts belonging to children must not receive advertisements, promoted content and content recommendations that designated SMSs are reasonably aware to be detrimental to children's physical or mental well-being.

Put in place tools for parents/guardians to manage their children's safety, such as tools to manage the content that their children view, the public visibility of their accounts, parties who can contact and interact with them and location sharing.

2. Empower Singapore users with effective and easy-to-use reporting mechanisms to report harmful content or unwanted interactions

Take appropriate action on user reports in a timely and diligent manner, and inform these users of their decision and any action taken in response to their reports.

3. Be accountable to Singapore users by providing transparency on their measures and levels of safety in annual online safety reports

Publish annual online safety reports online, to help users make an informed choice on which designated

23 "IMDA's Online Safety Code Comes Into Effect", *Infocomm Media Development Authority* (17 July 2024) <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/imdas-online-safety-code-comes-into-effect> (accessed 21 March 2025).

> SMS would be best placed to provide a safe user experience. … These annual online safety reports will provide information about measures designated SMSs have put in place to combat harmful content and how Singapore users' experience on the services has been.

(4) Enforcement and penalties

11 Designated online communication service providers must take all reasonably practicable steps to comply with the applicable code of practice.[24] If they fail to comply, IMDA can take regulatory action to order a financial penalty of any amount it thinks fit but not exceeding $1m[25] or direct them to take any steps, whether in or outside Singapore, and within a specified time to remedy the failure.[26] It should be noted that if a defaulting online communication service provider fails to comply with directions issued to it in relation to taking the reasonably practicable steps to remedy its failure of its duty,[27] it is guilty of an offence and is liable on conviction to a fine not exceeding $1m and a further fine not exceeding $100,000 for every day or part of a day during which the offence continues after conviction.[28]

12 It is immaterial whether the defaulting OCS is provided from within or outside of Singapore,[29] demonstrating the intention to capture offenders across jurisdictions.

B. Online Criminal Harms Act 2023

(1) Online content or activity criminal in nature

13 On the heels of OSMAA, the Online Criminal Harms Act 2023 ("OCHA") was introduced in May 2023 to help authorities deal more effectively with online content and activities that are criminal in nature.[30] This was the latest legislation to be

24 Broadcasting Act 1994 (2020 Rev Ed) s 45M.
25 Broadcasting Act 1994 (2020 Rev Ed) s 45N(1)(*a*).
26 Broadcasting Act 1994 (2020 Rev Ed) s 45N(1)(*b*).
27 Broadcasting Act 1994 (2020 Rev Ed) s 45M(1).
28 Broadcasting Act 1994 (2020 Rev Ed) s 45N(2).
29 Broadcasting Act 1994 (2020 Rev Ed) s 45N(3).
30 "Introduction of the Online Criminal Harms Bill", *Ministry of Home Affairs*, press release (8 May 2023) at para 1 <https://www.mha.gov.sg/mediaroom/

(cont'd on the next page)

introduced to combat various harms in the online space and better protect the public at large in Singapore, in addition to the Protection from Online Falsehoods and Manipulation Act 2019[31] and the Foreign Interference (Countermeasures) Act 2021.[32]

14 OCHA was deemed essential given how online spaces are being increasingly exploited by criminals. In Singapore, there were growing concerns over cases where voyeuristic images were being disseminated and sales of drugs occurred across a variety of online platforms.[33] For instance, 23 men were arrested in an operation against online child sexual exploitation, including for the transmission of obscene materials.[34] In 2022, 32 drug offenders were arrested in an operation against drug transactions conducted through chat apps.[35]

15 Further, scams and malicious cyber activities have also proliferated in recent years.[36] In 2022, 33,669 scams and

press-releases/introduction-of-the-online-criminal-harms-bill/> (accessed 21 March 2025).

31 2020 Rev Ed.

32 Act 28 of 2021. "Introduction of the Online Criminal Harms Bill", *Ministry of Home Affairs*, press release (8 May 2023) at para 1 <https://www.mha.gov.sg/mediaroom/press-releases/introduction-of-the-online-criminal-harms-bill/> (accessed 21 March 2025).

33 "Introduction of the Online Criminal Harms Bill", *Ministry of Home Affairs*, press release (8 May 2023) at para 2 <https://www.mha.gov.sg/mediaroom/press-releases/introduction-of-the-online-criminal-harms-bill/> (accessed 21 March 2025).

34 "Introduction of the Online Criminal Harms Bill", *Ministry of Home Affairs*, press release (8 May 2023) at para 2 <https://www.mha.gov.sg/mediaroom/press-releases/introduction-of-the-online-criminal-harms-bill/> (accessed 21 March 2025); "23 Men Arrested in Operation Targeting Online Child Sexual Exploitation Activities", *Singapore Police Force* (27 March 2023) <https://www.police.gov.sg/media-room/news/20230327_23_men_arr_in_op_targeting_online_child_sexual_exploitation_activities> (accessed 21 March 2025).

35 "Introduction of the Online Criminal Harms Bill", *Ministry of Home Affairs*, press release (8 May 2023) at para 2 <https://www.mha.gov.sg/mediaroom/press-releases/introduction-of-the-online-criminal-harms-bill/> (accessed 21 March 2025); "32 Suspected Drug Offenders Arrested for Drug Transactions Conducted on Chat Applications", *Central Narcotics Bureau* (20 April 2022) <https://www.cnb.gov.sg/NewsAndEvents/News/Index/32-suspected-drug-offenders-arrested-for-drug-transactions-conducted-on-chat-applications> (accessed 21 March 2025).

36 "Introduction of the Online Criminal Harms Bill", *Ministry of Home Affairs*, press release (8 May 2023) at para 3 <https://www.mha.gov.sg/mediaroom/press-releases/introduction-of-the-online-criminal-harms-bill/>

(cont'd on the next page)

cybercrime cases were reported in Singapore, a 25.2% increase from 2021, and more than $660m was lost to scams.[37] The most common scams, such as those offering attractive investments, jobs, and product deals, were often perpetrated or facilitated through online platforms. Phishing, which is often an attack vector for scams and malicious cyber activities, has also increased significantly. Approximately 8,500 phishing attempts were reported to Singapore Cyber Emergency Response Team ("SingCERT") in 2022, which is more than double the 3,100 phishing attempts reported in 2021.[38]

16 While there was a 52% decline in phishing attempts reported to SingCERT in 2023, this was still approximately 30% higher than the figures from 2021.[39] This defied a global trend of sharp increases, which were likely caused by the use of generative artificial intelligence (Gen AI) chatbots like ChatGPT to facilitate the production of phishing content at scale.[40] The Cyber Security Agency of Singapore ("CSA") has also observed that cybercriminals are shifting tactics to make their phishing attempts appear more legitimate and authentic, with more than

(accessed 21 March 2025); "32 Suspected Drug Offenders Arrested for Drug Transactions Conducted on Chat Applications", *Central Narcotics Bureau* (20 April 2022) <https://www.cnb.gov.sg/NewsAndEvents/News/Index/32-suspected-drug-offenders-arrested-for-drug-transactions-conducted-on-chat-applications> (accessed 21 March 2025).

37 "Annual Scams and Cybercrimes Brief 2022", *Singapore Police Force* <https://www.scamshield.gov.sg/files/Scams%20and%20Cybercrime%20Briefs/2022_annual_scams_and_cybercrime_brief.pdf>(accessed 21 March 2025).

38 "Introduction of the Online Criminal Harms Bill", *Ministry of Home Affairs*, press release (8 May 2023) at para 4 <https://www.mha.gov.sg/mediaroom/press-releases/introduction-of-the-online-criminal-harms-bill/> (accessed 21 March 2025).

39 "Fall in Phishing, Infected Infrastructure and Website Defacement Incidents Reported to CSA in 2023, But Absolute Figures Remain High", *Cyber Security Agency of Singapore*, press release (30 July 2024) at para 2 <https://www.csa.gov.sg/news-events/press-releases/fall-in-phishing--infected-infrastructure-and-website-defacement-incidents-reported-to-csa-in--2023--but-absolute-figures-remain-high> (accessed 21 March 2025).

40 "Fall in Phishing, Infected Infrastructure and Website Defacement Incidents Reported to CSA in 2023, But Absolute Figures Remain High", *Cyber Security Agency of Singapore*, press release (30 July 2024) at para 2 <https://www.csa.gov.sg/news-events/press-releases/fall-in-phishing--infected-infrastructure-and-website-defacement-incidents-reported-to-csa-in--2023--but-absolute-figures-remain-high> (accessed 21 March 2025).

half of the phishing uniform resource locators (URLs) being reported to the CSA using the more secure hypertext transfer protocol secure (HTTPS) protocol, which is a significant rise from the 9% in 2022.[41]

17 Concerningly, 63% of the organisations that were spoofed in reported phishing attempts were entities in the banking and financial services industry, which hold significant amounts of sensitive and valuable information including personal details and login credentials.[42]

(2) Directions against specified criminal offences

18 In the face of these dangers, OCHA allows for directions to be issued to online service providers, entities, or individuals, when there is reasonable suspicion that an online activity is in furtherance of the commission of an offence specified under the First Schedule to the OCHA.[43] The use of directions limits the reach of criminal online activities and prevents further exposure to the harm by Singapore users.[44]

19 In brief, there are five different directions that can be issued that designated officers[45] ("Designated Officers") can issue to any online service provider, entity, or individual, when there

41 "Fall in Phishing, Infected Infrastructure and Website Defacement Incidents Reported to CSA in 2023, But Absolute Figures Remain High", *Cyber Security Agency of Singapore*, press release (30 July 2024) at para 2 <https://www.csa.gov.sg/news-events/press-releases/fall-in-phishing--infected-infrastructure-and-website-defacement-incidents-reported-to-csa-in--2023--but-absolute-figures-remain-high> (accessed 21 March 2025).

42 "Fall in Phishing, Infected Infrastructure and Website Defacement Incidents Reported to CSA in 2023, But Absolute Figures Remain High", *Cyber Security Agency of Singapore*, press release (30 July 2024) at para 2 <https://www.csa.gov.sg/news-events/press-releases/fall-in-phishing--infected-infrastructure-and-website-defacement-incidents-reported-to-csa-in--2023--but-absolute-figures-remain-high> (accessed 21 March 2025).

43 "Introduction to OCHA", *Singapore Police Force* <https://www.police.gov.sg/Advisories/Online-Criminal-Harms-Act/Introduction-to-OCHA> (accessed 21 March 2025); Online Criminal Harms Act 2023 (Act 24 of 2023) Pt 2.

44 "Introduction to OCHA", *Singapore Police Force* <https://www.police.gov.sg/Advisories/Online-Criminal-Harms-Act/Introduction-to-OCHA> (accessed 21 March 2025); Online Criminal Harms Act 2023 (Act 24 of 2023) Pt 2.

45 See s 2 of the Online Criminal Harms Act 2023 (Act 24 of 2023), which defines "designated officer" as a designated officer appointed under s 4.

is reasonable suspicion that an online activity is in furtherance of the commission of a "specified offence"[46]:[47]

> (a) Stop Communication Direction. This requires the recipient of the direction to stop communicating specified online content (including substantially similar content) to people in Singapore. The recipients of the direction are persons and entities who communicated such online content.[48]
>
> (b) Disabling Direction. This requires online service providers to disable specified content (e.g. a post or page) on their service from the view of people in Singapore, which may include identical copies of the content.[49]
>
> (c) Access Blocking Direction. This requires internet service providers to block access to an online location such as a web domain from the view of people in Singapore.[50]
>
> (d) Account Restriction Direction. This requires online service providers to stop an account on their service from communicating in Singapore and/or interacting with people in Singapore.[51]
>
> (e) App Removal Direction. This requires app stores to remove an app from its Singapore storefront, to stop further downloads of the app by people in Singapore.[52]

20 At the initial stages, directions will be issued against scam websites and egregious online activities.[53] This approach enables the Government to prioritise tackling scams and egregious offences, while developing the necessary systems and processes to scale up the issuance of directions for online activities in

46 The specified offences are in Pt 1 of the First Schedule to the Online Criminal Harms Act 2023 (Act 24 of 2023).

47 "Commencement of the Online Criminal Harms Act (OCHA) on 1 February 2024", *Ministry of Home Affairs*, press release (30 January 2024) at para 6 <https://www.mha.gov.sg/mediaroom/press-releases/commencement-of-the-online-criminal-harms-act-ocha-on-1-february-2024/>(accessed 21 March 2025).

48 Online Criminal Harms Act 2023 (Act 24 of 2023) s 8.

49 Online Criminal Harms Act 2023 (Act 24 of 2023) s 9.

50 Online Criminal Harms Act 2023 (Act 24 of 2023) s 10.

51 Online Criminal Harms Act 2023 (Act 24 of 2023) s 11.

52 Online Criminal Harms Act 2023 (Act 24 of 2023) s 12.

53 "Commencement of the Online Criminal Harms Act (OCHA) on 1 February 2024", *Ministry of Home Affairs*, press release (30 January 2024) at para 7 <https://www.mha.gov.sg/mediaroom/press-releases/commencement-of-the-online-criminal-harms-act-ocha-on-1-february-2024/>(accessed 21 March 2025).

furtherance of the commission of other specified offences. Examples of egregious offences include, but are not restricted to, those related to threat of death and serious hurt, and threat to law-and-order.[54]

(3) Orders

21 If there is non-compliance with the directions issued, the competent authority[55] ("Competent Authority") may issue an order to restrict access to the service or part of the service, to limit the further exposure of persons in Singapore to the criminal activity.[56]

22 Importantly, orders are seen to operate alongside, and do not replace, other measures that the Government can take for the non-compliance of directions, such as prosecution.[57]

(4) Appeal framework

23 What then happens when parties wish to appeal? Recipients of a direction, the proprietor of the online location and the originator of the material targeted by the direction may apply to a Designated Officer for reconsideration.[58] For orders, the reconsideration of the Competent Authority may be sought.

---

54 "Commencement of the Online Criminal Harms Act (OCHA) on 1 February 2024", *Ministry of Home Affairs*, press release (30 January 2024) at para 7 <https://www.mha.gov.sg/mediaroom/press-releases/commencement-of-the-online-criminal-harms-act-ocha-on-1-february-2024/>(accessed 21 March 2025).

55 See s 2 of the Online Criminal Harms Act 2023 (Act 24 of 2023), which defines "competent authority" as competent authority appointed under s 3.

56 "Commencement of the Online Criminal Harms Act (OCHA) on 1 February 2024", *Ministry of Home Affairs*, press release (30 January 2024) at para 8 <https://www.mha.gov.sg/mediaroom/press-releases/commencement-of-the-online-criminal-harms-act-ocha-on-1-february-2024/>(accessed 21 March 2025); Online Criminal Harms Act 2023 (Act 24 of 2023) ss 28–31.

57 "Commencement of the Online Criminal Harms Act (OCHA) on 1 February 2024", *Ministry of Home Affairs*, press release (30 January 2024) at para 9 <https://www.mha.gov.sg/mediaroom/press-releases/commencement-of-the-online-criminal-harms-act-ocha-on-1-february-2024/>(accessed 21 March 2025); Online Criminal Harms Act 2023 (Act 24 of 2023) ss 28–31.

58 "Commencement of the Online Criminal Harms Act (OCHA) on 1 February 2024", *Ministry of Home Affairs*, press release (30 January 2024) at para 9 <https://www.mha.gov.sg/mediaroom/press-releases/commencement-

(cont'd on the next page)

24 Should the application for reconsideration be unsuccessful, the appellant can appeal to a "Reviewing Tribunal" for the direction or order to be cancelled.[59] The Reviewing Tribunal comprises a district judge or magistrate appointed by the President, on the advice of the Cabinet.[60]

(5) Power to require information

25 A Designated Officer, the Competent Authority or an authorised officer[61] may require any person to whom a direction or an order is issued to provide any information necessary for the administration of the Act.[62]

26 When there is a reasonable suspicion that a specified offence has been committed, police officers and enforcement officers can request online service providers or owners of online location(s) to provide relevant information to facilitate investigations and criminal proceedings.[63]

27 These powers also apply to entities that are based overseas and information that is stored overseas.[64]

---

of-the-online-criminal-harms-act-ocha-on-1-february-2024/>(accessed 21 March 2025); Online Criminal Harms Act 2023 (Act 24 of 2023) ss 35–36.

59 "Commencement of the Online Criminal Harms Act (OCHA) on 1 February 2024", *Ministry of Home Affairs*, press release (30 January 2024) at para 11 <https://www.mha.gov.sg/mediaroom/press-releases/commencement-of-the-online-criminal-harms-act-ocha-on-1-february-2024/>(accessed 21 March 2025); Online Criminal Harms Act 2023 (Act 24 of 2023) s 42.

60 Online Criminal Harms Act 2023 (Act 24 of 2023) s 38. See generally, Pt 8 of the Online Criminal Harms Act 2023 (Act 24 of 2023).

61 See s 2 of the Online Criminal Harms Act 2023 (Act 24 of 2023).

62 Online Criminal Harms Act 2023 (Act 24 of 2023) s 47.

63 "Commencement of the Online Criminal Harms Act (OCHA) on 1 February 2024", *Ministry of Home Affairs*, press release (30 January 2024) at para 14 <https://www.mha.gov.sg/mediaroom/press-releases/commencement-of-the-online-criminal-harms-act-ocha-on-1-february-2024/>(accessed 21 March 2025); Online Criminal Harms Act 2023 (Act 24 of 2023) s 48.

64 "Commencement of the Online Criminal Harms Act (OCHA) on 1 February 2024", *Ministry of Home Affairs*, press release (30 January 2024) at para 15 <https://www.mha.gov.sg/mediaroom/press-releases/commencement-of-the-online-criminal-harms-act-ocha-on-1-february-2024/>(accessed 21 March 2025).

III. Managing online harms in the face of challenges

A. Targeted approach in managing online harms

28 The legal framework set out thus far demonstrates a targeted approach to combating online harm whilst keeping individual rights in mind. For instance, OCHA allows for specific directions to be issued to Internet service providers such that access to harmful content must be blocked at the risk of sanctions.[65] This is an example of how Parliament has adopted a "better to be safe" approach when it comes to tackling the risks of criminal activities, as opposed to leaving things to chance.[66] It should also be pointed out that for certain types of harms, there is a lower threshold for issuance of directions given the increased need to protect the individuals involved.

29 Scams and malicious cyber-activities are often carried out through deception, with scammers creating online accounts or websites that seem authentic and legitimate.[67] Such accounts or websites are used to convinced victims to transit to another platform where they are then targeted for scams and asked to download malware that can steal their login credentials or other personal information.[68] Also, malicious actors often create thousands of blank websites in advance of a scam, coupled with domain names that resemble those of legitimate organisations.[69]

---

65 Online Criminal Harms Act 2023 (Act 24 of 2023) s 10.

66 "Second Reading of the Online Criminal Harms Bill", opening speech by Josephine Teo, Minister for Communications and Information & Second Minister for Home Affairs (5 July 2023) at para 4 <https://www.mha.gov.sg/mediaroom/parliamentary/second-reading-of-the-online-criminal-harms-bill/> (accessed 21 March 2025).

67 "Second Reading of the Online Criminal Harms Bill", opening speech by Josephine Teo, Minister for Communications and Information & Second Minister for Home Affairs (5 July 2023) at para 15 <https://www.mha.gov.sg/mediaroom/parliamentary/second-reading-of-the-online-criminal-harms-bill/> (accessed 21 March 2025).

68 "Second Reading of the Online Criminal Harms Bill", opening speech by Josephine Teo, Minister for Communications and Information & Second Minister for Home Affairs (5 July 2023) at para 15 <https://www.mha.gov.sg/mediaroom/parliamentary/second-reading-of-the-online-criminal-harms-bill/> (accessed 21 March 2025).

69 "Second Reading of the Online Criminal Harms Bill", opening speech by Josephine Teo, Minister for Communications and Information & Second Minister for Home Affairs (5 July 2023) at para 17 <https://www.mha.gov.

(cont'd on the next page)

When the malicious actors are ready to strike, these blank websites are swiftly activated, populated with scam content and pushed out to the public, who may fall prey within minutes.[70] It is for these reasons, where the ordinary thresholds of issuing directions may not be met, that legislation has deemed it necessary to set out a lower threshold for issuance of directions for scams and malicious cyber activity offences.[71]

30 An argument can be made that making it easier to issue directions in instances as such lends to the individual's interest of not being cheated or scammed. In any event, because there is no explicit right to information in Singapore, it is posited that the legal framework may appear paternalistic from the perspective of this author.

B. Challenges abound – scams

31 However, it should be noted that despite the approach through legislation, there are still challenges that arise. There are still concerning occurrences with scams that have come about. In 2023, scam victims in Singapore lost $651.8m, with a record high of over 46,000 cases being reported.[72] Notably, 73% of scam victims were aged below 50,[73] with young adults aged 20 to 29 mostly falling prey to job scams, while those aged 30 to 49

sg/mediaroom/parliamentary/second-reading-of-the-online-criminal-harms-bill/> (accessed 21 March 2025).

70 "Second Reading of the Online Criminal Harms Bill", opening speech by Josephine Teo, Minister for Communications and Information & Second Minister for Home Affairs (5 July 2023) at para 17 <https://www.mha.gov.sg/mediaroom/parliamentary/second-reading-of-the-online-criminal-harms-bill/> (accessed 21 March 2025).

71 Online Criminal Harms Act 2023 (Act 24 of 2023) s 6(1)(b).

72 Nadine Chua, "Scam Victims in S'Pore Lost $651.8m in 2023, with Record High of Over 46,000 Cases Reported", *The Straits Times* (18 February 2024) <https://www.straitstimes.com/singapore/courts-crime/scam-victims-in-s-pore-lost-6518m-in-2023-with-record-high-of-over-46000-cases-reported> (accessed 21 March 2025).

73 Nadine Chua, "Scam Victims in S'Pore Lost $651.8m in 2023, with Record High of Over 46,000 Cases Reported", *The Straits Times* (18 February 2024) <https://www.straitstimes.com/singapore/courts-crime/scam-victims-in-s-pore-lost-6518m-in-2023-with-record-high-of-over-46000-cases-reported> (accessed 21 March 2025).

mostly losing money to e-commerce scams.[74] Elderly aged 65 and above made up 7.1% of scam victims, with more than a third of them falling for fake friend call scams and over 13% falling for investment scams.[75]

32 Such incidents remind us about the transient nature of scams and online malicious behaviours. Indeed, the police have indicated that most online scams are perpetrated by scammers based outside Singapore and that such cases are difficult to investigate and prosecute.[76] Recovery of funds can be difficult especially when the money has already been transferred out of Singapore.[77] While there have successes with overseas law enforcement authorities in taking down scam syndicates, it is evident that legislation alone is not enough to prevent such online harms from happening.

33 In an operation with global police co-operation agency INTERPOL, the Anti-Scam Command ("ASCom"), which consolidates resources and expertise across all police units in Singapore, investigated over 2,000 individuals and froze more than 5,300 bank accounts in Singapore, recovering more than $11.5m.[78]

---

74 Nadine Chua, "Scam Victims in S'Pore Lost $651.8m in 2023, with Record High of Over 46,000 Cases Reported", *The Straits Times* (18 February 2024) <https://www.straitstimes.com/singapore/courts-crime/scam-victims-in-s-pore-lost-6518m-in-2023-with-record-high-of-over-46000-cases-reported> (accessed 21 March 2025).

75 Nadine Chua, "Scam Victims in S'Pore Lost $651.8m in 2023, with Record High of Over 46,000 Cases Reported", *The Straits Times* (18 February 2024) <https://www.straitstimes.com/singapore/courts-crime/scam-victims-in-s-pore-lost-6518m-in-2023-with-record-high-of-over-46000-cases-reported> (accessed 21 March 2025).

76 Nadine Chua, "Scam Victims in S'Pore Lost $651.8m in 2023, with Record High of Over 46,000 Cases Reported", *The Straits Times* (18 February 2024) <https://www.straitstimes.com/singapore/courts-crime/scam-victims-in-s-pore-lost-6518m-in-2023-with-record-high-of-over-46000-cases-reported> (accessed 21 March 2025).

77 Nadine Chua, "Scam Victims in S'Pore Lost $651.8m in 2023, with Record High of Over 46,000 Cases Reported", *The Straits Times* (18 February 2024) <https://www.straitstimes.com/singapore/courts-crime/scam-victims-in-s-pore-lost-6518m-in-2023-with-record-high-of-over-46000-cases-reported> (accessed 21 March 2025).

78 Nadine Chua, "Scam Victims in S'Pore Lost $651.8m in 2023, with Record High of Over 46,000 Cases Reported", *The Straits Times* (18 February 2024) <https://www.straitstimes.com/singapore/courts-crime/scam-victims-in-

(cont'd on the next page)

34 It is likely that the bad actors will relocate, whether physically or digitally, before the authorities can intervene, be it through legislation or criminal action. As it is, the bad actors are usually based overseas, engendering jurisdictional issues of intervention, enforcement and extraction.

C. Challenges abound – online radicalisation

35 Although legislations like OSMAA and OCHA were not enacted to directly combat online radicalisation, there is no denying that it is a key concern due to the prevalence of social media and its abuse. Complex issues are oversimplified on social media, without the proper background and context, leading to people often getting the wrong idea.[79] In 2023, a 15-year-old self-radicalised student thought about carrying out knife attacks and beheading non-Muslims in popular tourists areas was detained under the Internal Security Act 1960[80] ("ISA").[81] He was the youngest person to be detained under the ISA and was influenced by a foreign preacher, who has been banned from preaching in Singapore since 2015 for his segregationist teachings, while searching for religious content online.[82]

36 Another teenager, a 16-year-old, was convinced of far-right extremist content and was cautioned by the Internal Security Department to stay away from such content online, but

s-pore-lost-6518m-in-2023-with-record-high-of-over-46000-cases-reported> (accessed 21 March 2025).

79 Nadine Chua, "Online Radicalisation a Key Factor Driving Terror Threat in Singapore: Shanmugam", *The Straits Times* (updated 14 November 2024) <https://www.straitstimes.com/singapore/online-radicalisation-a-key-factor-in-driving-terror-threat-in-singapore-shanmugam>(accessed 21 March 2025).

80 2020 Rev Ed.

81 Jean Iau, "2 Teens Dealt With Under ISA; 15-Year-Old Student Is Youngest-Ever Detainee", *The Straits Times* (updated 22 November 2024) <https://www.straitstimes.com/singapore/two-teenagers-dealt-with-under-isa-including-15-year-old-who-is-youngest-ever-detainee>(accessed 21 March 2025).

82 Jean Iau, "2 Teens Dealt With Under ISA; 15-Year-Old Student Is Youngest-Ever Detainee", *The Straits Times* (updated 22 November 2024) <https://www.straitstimes.com/singapore/two-teenagers-dealt-with-under-isa-including-15-year-old-who-is-youngest-ever-detainee>(accessed 21 March 2025).

he did not do so.[83] He even went on the online gaming platform Roblox, joining multiple Islamic State in Iraq and Syria ("ISIS")-themed servers where the virtual game settings replicated ISIS conflict zones, such as those in Syria and Marawi city in southern Philippines, and taking on the role of "spokesperson" and "chief propagandist" in the game.[84] This was coupled with his intention to replicate his desire in real life.[85]

37 Whilst legislation such as OSMAA and OCHA can provide safety parameters within which users are meant to operate within the online space, it is evident that it cannot shield its users from everything online, including that of simplified complex content that may lead to online radicalisation as explored above. If anything, the challenge of online radicalisation demonstrates that legislating against online harms alone is insufficient to combat the dangers of the online space.

IV. What else can be done

A. Not one solution

38 It is evident that managing online harms is not a "one and done" solution. ASCom constantly monitors trends in scam variants and has ironically even relied on artificial intelligence in combating these challenges in technology.[86] ASCom identifies the

83 Jean Iau, "2 Teens Dealt With Under ISA; 15-Year-Old Student Is Youngest-Ever Detainee", *The Straits Times* (updated 22 November 2024) <https://www.straitstimes.com/singapore/two-teenagers-dealt-with-under-isa-including-15-year-old-who-is-youngest-ever-detainee>(accessed 21 March 2025).

84 Jean Iau, "2 Teens Dealt With Under ISA; 15-Year-Old Student Is Youngest-Ever Detainee", *The Straits Times* (updated 22 November 2024) <https://www.straitstimes.com/singapore/two-teenagers-dealt-with-under-isa-including-15-year-old-who-is-youngest-ever-detainee>(accessed 21 March 2025).

85 Jean Iau, "2 Teens Dealt With Under ISA; 15-Year-Old Student Is Youngest-Ever Detainee", *The Straits Times* (updated 22 November 2024) <https://www.straitstimes.com/singapore/two-teenagers-dealt-with-under-isa-including-15-year-old-who-is-youngest-ever-detainee>(accessed 21 March 2025).

86 Koh Wan Ting, "'Not One and Done': How Singapore's Police and Government Tech Agency Combat Ever-Evolving Scams", *CNA* (updated 4 March 2025)

(cont'd on the next page)

trending scams on a daily and weekly basis before allocating the necessary resources and coming up with ways to tackle them.[87]

39 Dealing with online harms like scams is a cat-and-mouse game, with the Singapore Government's principal product manager in anti-scam products, the Government Technology Agency of Singapore ("GovTech"), fighting an "ongoing battle".[88] A tool that runs in the background would not be effective in combating scams as scammers react quickly and use evasion techniques. For instance, once a swindler is given accessibility access to a phone, they "will take over to grant other permissions, which flash across the screen in a series of lightning-fast pop-ups".[89]

40 Alongside existing legislation, GovTech and the Ministry of Home Affairs ("MHA") have rolled out anti-scam products to take down hoax websites masquerading as official ones.[90] For instance, the Scam Analytics and Tactical Intervention System (SATIS) both hunts and disrupts scam sites and has expanded beyond government websites to include bank phishing sites, sites hosting malware and those used in impersonation scams.[91]

<https://www.channelnewsasia.com/singapore/scams-spf-govtech-technology-4144416> (accessed 21 March 2025).

87 Koh Wan Ting, "'Not One and Done': How Singapore's Police and Government Tech Agency Combat Ever-Evolving Scams", *CNA* (updated 4 March 2025) <https://www.channelnewsasia.com/singapore/scams-spf-govtech-technology-4144416> (accessed 21 March 2025).

88 Koh Wan Ting, "'Not One and Done': How Singapore's Police and Government Tech Agency Combat Ever-Evolving Scams", *CNA* (updated 4 March 2025) <https://www.channelnewsasia.com/singapore/scams-spf-govtech-technology-4144416> (accessed 21 March 2025).

89 Koh Wan Ting, "'Not One and Done': How Singapore's Police and Government Tech Agency Combat Ever-Evolving Scams", *CNA* (updated 4 March 2025) <https://www.channelnewsasia.com/singapore/scams-spf-govtech-technology-4144416> (accessed 21 March 2025).

90 Koh Wan Ting, "'Not One and Done': How Singapore's Police and Government Tech Agency Combat Ever-Evolving Scams", *CNA* (updated 4 March 2025) <https://www.channelnewsasia.com/singapore/scams-spf-govtech-technology-4144416> (accessed 21 March 2025).

91 Koh Wan Ting, "'Not One and Done': How Singapore's Police and Government Tech Agency Combat Ever-Evolving Scams", *CNA* (updated 4 March 2025) <https://www.channelnewsasia.com/singapore/scams-spf-govtech-technology-4144416> (accessed 21 March 2025).

41 Given the adeptness of scammers, would further legislation to increase police powers be part of the solution? Recently, the MHA announced that it would be introducing the Protection from Scams Bill[92] ("Bill"), which seeks to empower the police to issue restriction orders ("RO") "to temporarily restrict the banking transactions of targets of ongoing scams who refuse to believe that they are being scammed".[93] ROs will only be issued for scams that are conducted via digital or telecommunication channels where there have not been any in-person interactions,[94] demonstrating the type of offence that they intend to target. Issued as a last resort,[95] ROs will stop money transfers and suspend all credit facilities when issued. If an individual has been assessed to warrant an RO, the police will issue the RO to all seven domestic systemically important banks (D-SIBs) in Singapore, in case the individual has banking accounts with more than one bank.[96] ROs are valid for a period of 28 days in the first instance[97] and subject to further renewal by the police for up to 28 days at a time.[98]

92 Bill No 43/2024.

93 "Public Consultation on Protection From Scams Bill", *Ministry of Home Affairs*, press release (30 August 2024) at para 1 <https://www.mha.gov.sg/mediaroom/press-releases/public-consultation-on-protection-from-scams-bill/> (accessed 21 March 2025).

94 "Public Consultation on Protection From Scams Bill", *Ministry of Home Affairs*, press release (30 August 2024) at para 6 <https://www.mha.gov.sg/mediaroom/press-releases/public-consultation-on-protection-from-scams-bill/> (accessed 21 March 2025).

95 "Public Consultation on Protection From Scams Bill", *Ministry of Home Affairs*, press release (30 August 2024) at para 12 <https://www.mha.gov.sg/mediaroom/press-releases/public-consultation-on-protection-from-scams-bill/> (accessed 21 March 2025).

96 "Public Consultation on Protection From Scams Bill", *Ministry of Home Affairs*, press release (30 August 2024) at para 9(c) <https://www.mha.gov.sg/mediaroom/press-releases/public-consultation-on-protection-from-scams-bill/> (accessed 21 March 2025).

97 "Public Consultation on Protection From Scams Bill", *Ministry of Home Affairs*, press release (30 August 2024) at para 10 <https://www.mha.gov.sg/mediaroom/press-releases/public-consultation-on-protection-from-scams-bill/> (accessed 21 March 2025).

98 "Public Consultation on Protection From Scams Bill", *Ministry of Home Affairs*, press release (30 August 2024) at para 11 <https://www.mha.gov.sg/mediaroom/press-releases/public-consultation-on-protection-from-scams-bill/> (accessed 21 March 2025).

42 Importantly, the Bill seeks to strike a balance between protecting the public from scams, and not unduly inconveniencing the individual beyond what is necessary to protect them and maintaining a sense of personal responsibility and choice.[99] This is vital because whilst legislation and enforcement can set parameters and intervene where necessary, the individual needs to remain vigilant as the first line of defence against ill actors. Public consultation for the Bill closed on 30 September 2024.

B. Urging accountability

43 "Ultimately, aspirational measures to tackle online harms, no matter how laudable, will only be as strong as their legal enforcement."[100] Policymakers as well as the public at large need to constantly equip themselves with the relevant technical knowledge about online harms and how to cope with them, to anticipate new risks.[101] As law enforcement in Singapore has been doing its best to cope, policymakers have to continue to hold big tech companies accountable at each stage of their product designs and implementation, with a view to protecting the public.[102]

44 An example of how such accountability is manifested is seen in how Minister of State for Home Affairs Sun Xueling called out Meta's lack of co-operation with the Singapore government when it came to combatting scams.[103] She identified how Meta had

99 "Public Consultation on Protection From Scams Bill", *Ministry of Home Affairs*, press release (30 August 2024) at para 8 <https://www.mha.gov.sg/mediaroom/press-releases/public-consultation-on-protection-from-scams-bill/> (accessed 21 March 2025).

100 Sean Tan, "Regulating Online Harms: Are Current Efforts Working – Or Even Workable?", *RSIS Commentary* (23 November 2023) <https://rsis.edu.sg/wp-content/uploads/2023/11/CO23170.pdf> (accessed 21 March 2025).

101 Sean Tan, "Regulating Online Harms: Are Current Efforts Working – Or Even Workable?", *RSIS Commentary* (23 November 2023) <https://rsis.edu.sg/wp-content/uploads/2023/11/CO23170.pdf> (accessed 21 March 2025).

102 Sean Tan, "Regulating Online Harms: Are Current Efforts Working – Or Even Workable?", *RSIS Commentary* (23 November 2023) <https://rsis.edu.sg/wp-content/uploads/2023/11/CO23170.pdf> (accessed 21 March 2025).

103 Louisa Tang, "'Do Right By Your Users': Sun Xueling Criticises Meta For Not Doing Enough to Fight Facebook Scams", *CNA* (29 February 2024) <https://www.channelnewsasia.com/singapore/facebook-meta-criticised-not-doing-enough-fight-scams-sun-xueling-4158831> (accessed 21 March 2025).

"consistently pushed back" against the MHA's recommendations to put in place safeguards against scams on the social media platform.[104] Out of a total of 9,783 e-commerce scams reported in Singapore during 2023, close to half of the scams were on Facebook.[105] Facebook is the only platform in the E-commerce Marketplace Transaction Safety Ratings ("TSR") that has not implemented, or started to implement, recommended safety features, resulting in it being ranked the lowest in the TSR for the second consecutive year.[106] This is in comparison with platforms like Shopee, which introduced verification features in December 2022 where sellers were required to verify their identities against government records. Scams reported on the e-commerce platform fell 71% between 2021 and 2023 as a result.[107]

45 While such public name shaming might not lead to immediate changes, it is important that authorities do its part to commend its partners who comply with its safety recommendations and call out those who fail to, to ensure a safe online space for its users. This is essential given that SMSs are whom and through whom users interact with when accessing content online.

104 Louisa Tang, "'Do Right By Your Users': Sun Xueling Criticises Meta For Not Doing Enough to Fight Facebook Scams", *CNA* (29 February 2024) <https://www.channelnewsasia.com/singapore/facebook-meta-criticised-not-doing-enough-fight-scams-sun-xueling-4158831> (accessed 21 March 2025).

105 Louisa Tang, "'Do Right By Your Users': Sun Xueling Criticises Meta For Not Doing Enough to Fight Facebook Scams", *CNA* (29 February 2024) <https://www.channelnewsasia.com/singapore/facebook-meta-criticised-not-doing-enough-fight-scams-sun-xueling-4158831> (accessed 21 March 2025).

106 Louisa Tang, "'Do Right By Your Users': Sun Xueling Criticises Meta For Not Doing Enough to Fight Facebook Scams", *CNA* (29 February 2024) <https://www.channelnewsasia.com/singapore/facebook-meta-criticised-not-doing-enough-fight-scams-sun-xueling-4158831> (accessed 21 March 2025).

107 Louisa Tang, "'Do Right By Your Users': Sun Xueling Criticises Meta For Not Doing Enough to Fight Facebook Scams", *CNA* (29 February 2024) <https://www.channelnewsasia.com/singapore/facebook-meta-criticised-not-doing-enough-fight-scams-sun-xueling-4158831> (accessed 21 March 2025).

C. Being vigilant of trending criminal harms

46 The plain fact is that technology-based solutions cannot address zero-day vulnerabilities and there needs to be greater ownership of user responsibility and public education for the public to stay ahead of trending online criminal harms.[108] Every individual needs to keep abreast of the harms being perpetuated online so that they are aware when they may be falling prey to them. This personal responsibility towards safety works in tandem with the efforts of authorities.

47 One uniquely Singaporean way in which this joint effort has manifested is seen in the Shared Responsibility Framework ("SRF") which was launched by the Monetary Authority of Singapore and IMDA and came into force on 16 December 2024.[109] SRF assigns financial institutions ("FIs") and telecommunication companies duties to mitigate phishing scams, and sets expectations of payouts to affected scam victims when these duties are breached.[110] To better protect consumers, SRF introduces five duties for FIs:

> (a) Cooling off period: FIs must impose a cooling off period of at least 12 hours during which high-risk activities cannot be performed when a digital security token is activated on a device or when there is a login to a protected account on a new device.[111]

---

108 See Andy Greenberg, "Andy Greenberg, 'Inside a Firewall Vendor's 5-Year War With the Chinese Hackers Hijacking Its Devices', *Wired* (31 October 2024) <https://www.wired.com/story/sophos-chengdu-china-five-year-hacker-war/> (accessed 21 March 2025).

109 "MAS and IMDA Announce Implementation of Shared Responsibility Framework from 16 December 2024", *Monetary Authority of Singapore*, media release (24 October 2024) at para 1 <https://www.mas.gov.sg/news/media-releases/2024/mas-and-imda-announce-implementation-of-shared-responsibility-framework-from-16-december-2024> (accessed 21 March 2025).

110 "MAS and IMDA Announce Implementation of Shared Responsibility Framework from 16 December 2024", *Monetary Authority of Singapore*, media release (24 October 2024) at para 2 <https://www.mas.gov.sg/news/media-releases/2024/mas-and-imda-announce-implementation-of-shared-responsibility-framework-from-16-december-2024> (accessed 21 March 2025).

111 Guidelines on Shared Responsibility Framework at para 4.2.1.

(b) Notification alerts: FIs must provide notification alerts, on a real-time basis, to account holders when a digital security token is activated, there is a login to a protected account on a new device, or when any high-risk activities are performed on a protected account.[112]

(c) Outgoing transaction alerts:[113] FIs must provide notification alerts, on a real-time basis, of all outgoing payment transactions made from the account holder's protected account.

(d) Reporting channel and self-service feature:[114] FIs must provide a reporting channel available for prompt reporting and blocking of further seemingly authorised transactions. This channel must include a self-service feature to promptly block further mobile and online access to the protected account.

(e) Real-time fraud surveillance:[115] FIs must have real-time fraud surveillance to detect seemingly authorised transactions. If a protected account is rapidly drained of a material sum, the FI must (i) block the transaction that would cross a set threshold and all subsequent transactions to the scammer until further verification from the account holder is obtained; or (ii) send a notification, and block or hold the transaction for at least 24 hours.

48 The SRF operates as part of the broader suite of upstream and downstream measures that authorities and stakeholders have progressively implemented to tackle scams in Singapore.[116]

112 Guidelines on Shared Responsibility Framework at para 4.2.2.
113 Guidelines on Shared Responsibility Framework at para 4.2.3.
114 Guidelines on Shared Responsibility Framework at para 4.2.4.
115 Guidelines on Shared Responsibility Framework at para 4.2.5.
116 "MAS and IMDA Announce Implementation of Shared Responsibility Framework from 16 December 2024", *Monetary Authority of Singapore*, media release (24 October 2024) at para 4 <https://www.mas.gov.sg/news/media-releases/2024/mas-and-imda-announce-implementation-of-shared-responsibility-framework-from-16-december-2024> (accessed 21 March 2025).

Apart from the SRF, banks also have their respective discretionary goodwill frameworks to support scam victims.[117]

49 Ultimately, it is vital that authorities also keep a keen eye on any trends in terms of online harm to react better to it. In 2022, there were 179 technology-facilitated cases of sexual violence, with 28% occurring on messaging platforms such as Telegram and WhatsApp, and 19% occurring on social media platforms like Facebook and TikTok.[118] It is a concern that technology-facilitated sexual violence is growing more complex and that "with increasingly sophisticated encrypted platforms and generative artificial intelligence, victims may not only find themselves unknowingly featured in explicit content, but also face difficulty in securing evidence and reporting such advanced forms of online harms".[119]

50 A 2024 survey by the Ministry of Digital Development and Information found that 66% of respondents encountered harmful content in SMSs designated by the IMDA under the Code of Practice [120] Of these respondents, 61% ignored it, 35% blocked the offending account or user, and only 27% reported it to the platform.[121] Overall, 74% of respondents in the 2024 survey

117 "MAS and IMDA Announce Implementation of Shared Responsibility Framework from 16 December 2024", *Monetary Authority of Singapore*, media release (24 October 2024) at para 4 <https://www.mas.gov.sg/news/media-releases/2024/mas-and-imda-announce-implementation-of-shared-responsibility-framework-from-16-december-2024> (accessed 21 March 2025).

118 Syarafana Shafeeq, "No Recent Spike in Tech-Facilitated Sexual Harm, But AI Poses Concern for Future: Women's Groups", *The Straits Times* (28 January 2024) <https://www.straitstimes.com/singapore/no-recent-spike-in-tech-facilitated-sexual-harm-but-ai-poses-concern-for-future-women-s-groups> (accessed 21 March 2025).

119 Syarafana Shafeeq, "No Recent Spike in Tech-Facilitated Sexual Harm, But AI Poses Concern for Future: Women's Groups", *The Straits Times* (28 January 2024) <https://www.straitstimes.com/singapore/no-recent-spike-in-tech-facilitated-sexual-harm-but-ai-poses-concern-for-future-women-s-groups> (accessed 21 March 2025).

120 "MDDI Survey: Two Thirds of Respondents Encountered Harmful Online Content", *Ministry of Digital Development and Information* (25 July 2024) at para 1 <https://www.mddi.gov.sg/media-centre/press-releases/mddi-survey-two-thirds-respondents-encountered-harmful-online-content/> (accessed 21 March 2025).

121 "MDDI Survey: Two Thirds of Respondents Encountered Harmful Online Content", *Ministry of Digital Development and Information* (25 July 2024)

(cont'd on the next page)

encountered harmful online content (an increase from 64% in 2023), with 66% encountering harmful content in designated SMSs (an increase from 57% in 2023).[122]

51 Ideally, legislators should bear such trends in mind and adapt, amending and enacting legislation where required. It was announced that new legislation and measures will be introduced to help combat online harms and provide stronger assurance to victims.[123] This is in recognition of how all victims of online harms would want damaging content to be removed quickly and permanently and that current legal and criminal measures can take time.[124] The upcoming dedicated agency will support victims of online harms in seeking more timely and effective relief.[125] The idea is to introduce a complaints mechanism which will be administered by the new agency to provide timely assistance to victims of online harms.[126] The agency will also introduce statutory torts for various online harms, to provide legal certainty where victims of such harms choose to pursue

at para 1 <https://www.mddi.gov.sg/media-centre/press-releases/mddi-survey-two-thirds-respondents-encountered-harmful-online-content/> (accessed 21 March 2025).

122 "MDDI Survey: Two Thirds of Respondents Encountered Harmful Online Content", *Ministry of Digital Development and Information* (25 July 2024) at para 3 <https://www.mddi.gov.sg/media-centre/press-releases/mddi-survey-two-thirds-respondents-encountered-harmful-online-content/> (accessed 21 March 2025).

123 Lawrence Wong, Prime Minister and Minister for Finance, speech at the launch of Smart Nation 2.0 (1 October 2024) <https://www.pmo.gov.sg/Newsroom/PM-Lawrence-Wong-at-the-Launch-of-Smart-Nation> (accessed 21 March 2025).

124 Lawrence Wong, Prime Minister and Minister for Finance, speech at the launch of Smart Nation 2.0 (1 October 2024) <https://www.pmo.gov.sg/Newsroom/PM-Lawrence-Wong-at-the-Launch-of-Smart-Nation> (accessed 21 March 2025).

125 Lawrence Wong, Prime Minister and Minister for Finance, speech at the launch of Smart Nation 2.0 (1 October 2024) <https://www.pmo.gov.sg/Newsroom/PM-Lawrence-Wong-at-the-Launch-of-Smart-Nation> (accessed 21 March 2025).

126 Zhaki Abdullah, "More Ways Proposed For Victims of Online Harms to Seek Redress, Including Getting Content Blocked", *The Straits Times* (updated 22 November 2024) <https://www.straitstimes.com/singapore/broader-measures-proposed-for-victims-of-online-harms-including-getting-access-to-content-disabled> (accessed 21 March 2025).

redress against perpetrators to hold them accountable through liability for online harms.[127]

V. Conclusion

52 Ultimately, tackling harmful online content requires a whole-of-society effort.[128] While legislation like OSMAA and OCHA are patently positive steps in the right direction, preventing online harms is not just about legislation nor is it about the enforcement of the individual's rights. It is also about inculcating responsibility in individuals to learn about online harms and how they are perpetuated, and how they can stay safe whilst navigating the Internet. Arguably, mediating the balance between managing online criminal harms and the rights of the individual requires a constant vigilant effort in adapting to the different challenges brought by bad actors in the online space. Non-complying SMSs, for instance, should be called out publicly and encouraged to "step up" their game to ensure a safe space for its users. Rightly, authorities should provide necessary support and incentives for compliance, coupled with sanctions where there is continued non-compliance.

53 OSMAA and OCHA are important steps towards creating a safer online space for Singapore users, particularly the vulnerable, that of children. Legislation provides a framework within which users may operate safely, if all involved, be it operators or users, abide by the safety recommendations and protocols. On the part of the user, we need to continue to do our part offline as well to be aware and reduce the possibility and extent of harm that may be caused.

127 Zhaki Abdullah, "More Ways Proposed For Victims of Online Harms to Seek Redress, Including Getting Content Blocked", *The Straits Times* (updated 22 November 2024) <https://www.straitstimes.com/singapore/broader-measures-proposed-for-victims-of-online-harms-including-getting-access-to-content-disabled> (accessed 21 March 2025).

128 "First Reading of Online Safety (Miscellaneous Amendments) Bill", *Ministry of Digital Development and Information*, press release (3 October 2022) at para 14 <https://www.mddi.gov.sg/media-centre/press-releases/first-reading-of-online-safety-bill/> (accessed 21 March 2025).