SQUIRE PATTON BOGGS

Singapore's Online Safety (Relief and Accountability) Bill: Key Insights

APAC – December 2025

On 5 November 2025, the Online Safety (Relief and Accountability) Bill (the Bill) was passed by the Singapore Parliament. It will come into force on a future date to be appointed by the minister by notification in the Gazette.

The Bill introduces a new and improved regulatory framework in Singapore to protect and empower victims of online harm, establish the Office of the Commissioner of Online Safety (Commissioner), deter and prevent online harmful activity, and give victims the right, in some circumstances, to claim directly against online platforms for specified harms.

Key Provisions

Establishment of the OSC

The Bill will establish the Online Safety Commission (OSC) as a statutory body responsible for administering the Bill and providing remedies to victims who report online harm.

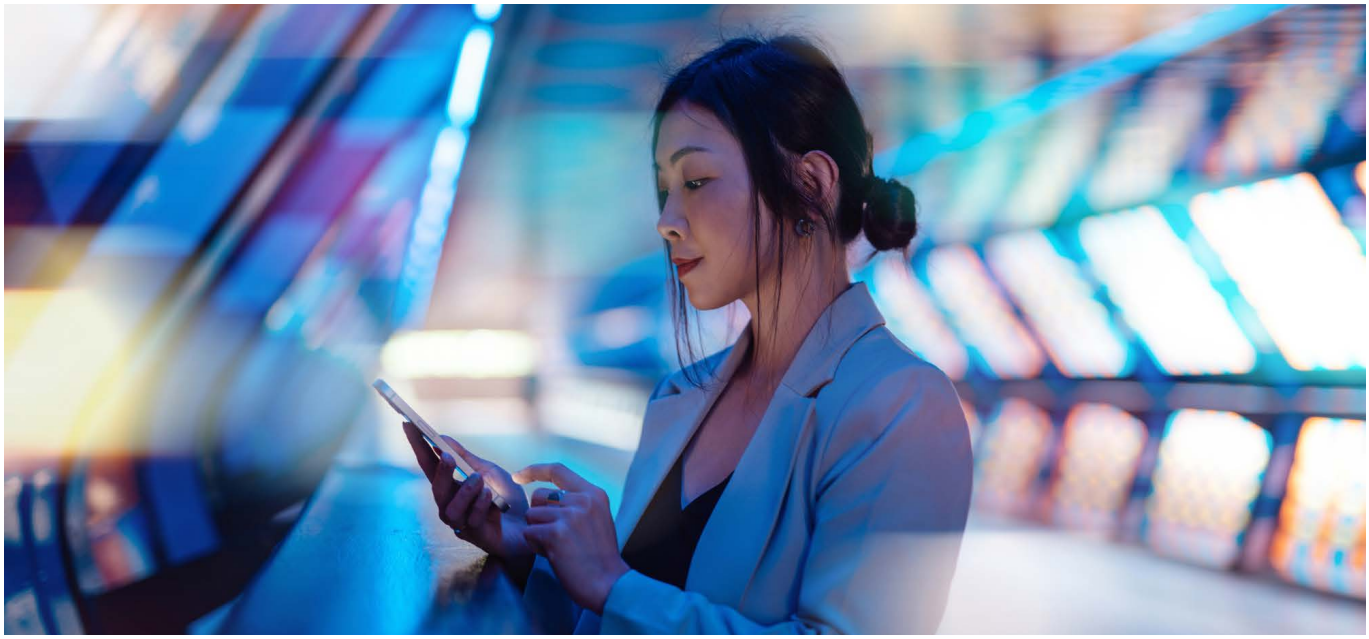
Insight – The establishment of an OSC clearly signals the importance to the Singapore government in tackling online harm. Unlike the Australian regime, the Bill only permits the Commissioner to act or investigate alleged online harm upon receiving a report – whereas the eSafety Commissioner may investigate on their own volition.

Categories of Online Harm

The OSC will cover the 13 categories of online harmful activity under the Bill, being **online harassment**, **doxxing**, **online stalking**, **intimate image abuse**, **image-based child abuse**, nonconsensual disclosure of private information, online impersonation, inauthentic material abuse, publication of false material, publication of statements harmful to reputation, online instigation of disproportionate harm, incitement of enmity and incitement of violence.

Insight – This is a wide scope, and some of the harms listed – including inauthentic material abuse and online instigation of disproportionate harm – are not directly prohibited under Australian and UK online safety law, perhaps reflecting that Singapore is a more culturally conservative country. However, like Australia and the UK, Singapore is taking a phased approach to implementation, with only the categories of harms in **bold** above taking effect now.

It is also worth remarking that certain of these actions – such as nonconsensual disclosure of private information and publication of false material – are likely to overlap with existing rights available to individuals in Singapore, including under the Personal Data Protection Act (PDPA) and defamation law. It is unclear how victims will choose to frame their claims and whether they can bring actions under different laws concurrently.



Powers of the Commissioner

Upon receiving a report of online harmful activity from an eligible victim,[1] the Commissioner may make one or more of the following directions under Part 5 of the Act if the Commissioner is satisfied that the online harmful activity has occurred:

Direction	Recipient
Stop communication direction – This requires the recipient to remove relevant material, stop disseminating the material or remove the relevant location so that the material or location can no longer be accessed by persons in Singapore.	Communicator of the relevant material (Communicator), who is not an administrator or online service provider (OSP) (defined below). Administrator of the relevant location at which the relevant material is communicated (Administrator). "Administrator" is defined to include any entity that develops, maintains, organises, manages, supervises, regulates access to, or exercises editorial control over an online location (such as a website or chat group). This excludes entities like OSPs or internet access providers merely hosting the location.
Stop communication with respect to a specified class of material direction – This operates as above but it covers a class of material and may, therefore, even apply to material which is published after a direction is made.	• Communicator • Administrator
Restraining direction – The recipient must refrain from certain specified activity, e.g. communicating material similar or identical to the proscribed material.	Communicator, Administrator and the individual who actually conducted the relevant activity, e.g. the individual who has posted the relevant material online.
Access disabling direction – This requires an OSP blocking access by Singapore end-users to specific material.	OSP, where the online service provided is not an internet access or app distribution service, each of which are regulated separately.
Access disabling with respect to a specified class of material direction – See above, but for a class of material.	OSP that has been prescribed under the regulations.
Right of reply (user) direction – A recipient must communicate a reply notice alongside the relevant material or, where appropriate, alongside material substantially similar to the relevant material.	• Communicator • Administrator
Right of reply (online service) direction – See above, but for an OSP, which must also make sure that the reply notice is "easily perceived" (which is defined prescriptively).	OSP
Labelling direction – This requires the publication of a notice at a location, indicating that Part 5 directions have been issued.	Administrator
Account restriction direction – The recipient must disallow or restrict the access or interaction of a specific account or disable the account.	Administrator and OSP
Engagement reduction direction – The recipient must reduce the engagement of end users in Singapore with the relevant class of harmful material, which must be identified in the direction by a "specific identifier" to be effective (e.g. username).	OSP

In the event of a noncompliance with a direction, the OSC may make an order blocking access or removing an app. Failure to comply with directions and orders may result in criminal liability.

1 The individual must be a citizen of Singapore, a permanent resident of Singapore; or a person who has a prescribed connection to Singapore. The detail of the last category is still to be determined, but the second reading speech confirmed that it will include foreign visitors who are staying on a long-term basis in Singapore, including foreign spouses who are in Singapore on a long-term visa pass.

Insight – Many of these directions involve new powers that have been tailored to the specific online harm. For example, the OSC may only order a right-of-reply notice in relation to the publication of false material or a statement harmful to a person's reputation, or an online instigation of disproportionate harm.

Insight – Overseas enforcement is a good indicator as to how some of these powers will be exercised in Singapore. In 2024, the Australian eSafety Commissioner issued a removal notice[2] against X Corp in 2024, requiring that X "take all reasonable steps" to remove a video that contained real violence. Rather than removing it, X "geo-blocked" the material so that it could no longer be accessed from an Australian IP address.

The Federal Court did not accept the eSafety Commissioner's argument that X should be compelled to remove the content and held that X's decision to geo-block the content was "reasonable" in the context of the Australian law.[3] It is likely that the Singapore Commissioner will take a similar approach, especially as the power to issue a stop direction is expressly defined to mean blocking access to users in Singapore.[4] While there are obvious means to circumvent such a direction (e.g. VPN), there are also ways for a regulator or platforms to monitor such circumvention – albeit involvinwg the collection of significant personal data.

Statutory Torts Framework

In addition to an individual's right to complain to the OSC, the statutory torts framework under Part 10 of the Bill provides victims with a statutory right to bring civil proceedings directly against the perpetrator, to claim damages (such as for loss of future earnings and loss of earning capacity) and other heads of loss, such as an injunction or an account of profits.

Victims are entitled to seek relief in the courts for serious online harms, such as intimate image abuse, image-based child abuse, online impersonation, inauthentic material abuse, online instigation of disproportionate harm and incitement of violence.

Notably, the Bill also empowers a court to award enhanced damages to a victim in certain circumstances, including where a respondent failed reasonably to address online harmful activity reasonably notified to them by the victim.[5]

Insight – There are no such statutory torts under Australian or UK online safety law, both of which focus on regulatory powers. The closest that Australia has come is the new statutory tort for serious invasions of privacy, which was introduced into the *Privacy Act 1988* (Cth) earlier this year.

While courts are empowered under Part 13 of the Bill to award any damages that they consider to be "just and equitable", there is no explicit reference to damages for emotional harm and distress. In our experience, these are the kinds of noneconomic losses most likely to be suffered by victims of online harm, and they can be difficult to establish. However, the Singapore Court of Appeal recently held[6] that "loss or damage" under the PDPA could include damages for emotional distress, suggesting that Singapore courts may be more willing to award such damages where certain circumstances apply.

Statutory Duties

Parts 11 and 12 of the Bill also impose various duties on different members of the "tech stack", also in the form of statutory torts. For example:

(b) An Administrator has a duty to not develop or maintain an online location in a manner that facilitates or permits online harm to take place, assuming that it either intends for online harm to take place or at least has knowledge that such online harm is likely to be conducted. "Knowledge" appears to be defined objectively, with relevant factors including the profile of users at a location and the purpose for which the location is used or administered.

(c) Both an Administrator and an OSP must, if sent an online harms notice, take reasonable care to assess whether the applicable harmful activity has occurred and, if so, take reasonable steps to address it. Acting "reasonably" will turn on the facts of each situation.

Insight – This is a new and significant development. Nothing equivalent exists under UK or Australian online safety law, although the Australian government is currently seeking feedback on how to best design a digital duty of care into the Online Safety Act.

Ultimately, the statutory torts under the Bill are powerful, but many only activate upon receiving notice of online harm (or, given their nature, require an individual to first bring a claim). They do not require platforms to proactively scan for all harm but instead regulate how the platforms respond. This appears to be different from the proposed Australian model digital duty of care (although this is not in yet in force), which may place the onus on digital platforms to prevent online harms.

2 See eSafety Commissioner's Statement on Removal of Extreme Violent Content.

3 See *eSafety Commissioner v X Corp* [2024] FCA 499.

4 Section 29.

5 Section 98(1).

6 See *Michael Reed v Alex Bellingham and Attorney-General, intervener* [2022] SGCA 60.

End-user ID

Finally, Part 6 of the Bill grants the OSC broad powers to obtain information and documents, including identity information of an end user that is in the possession of platforms, and also require platforms to take reasonable steps to obtain specified information that may identify the user. Relevantly, the OSC is authorised to disclose the perpetrator's identity information to a victim for the purposes of enabling them to bring their claim or for other purposes such as allowing victims to safeguard themselves and take proactive measures.

Insight – These provisions enabling end-user identification and disclosure to victims are intended to address the problem of perpetrators exploiting anonymity to cause online harm. However, they also risk inappropriate or excessive disclosure of personal data. Among other requirements, the OSC may only exercise these powers where it reasonably suspects that an end user has engaged in harmful online activity. While the exercise will typically be justified under the PDPA as data processing that is required by law, it is critical that the power is only exercised in limited circumstances, and that any data shared with either victims or the OSC is limited to the minimum amount necessary.

Conclusion

As we wait for the Bill to become law, we recommend that digital platforms do the following:

- Establish whether you fall within any of the categories of actors that are regulated by the Bill, including whether you are an Administrator, Communicator or OSP.
- Assess and, where necessary, improve reporting pipelines so that platforms are empowered to respond to the OSC in the extremely short timelines imposed by the Bill.
- If you are a global platform, be aware that the threshold for directions to remove certain content is much lower in Singapore than, potentially, other countries in which you operate, and that the OSC's powers extend beyond take-down notices to, among other things, orders to correct or reduce engagement with material. Consider ways of complying with OSC orders without compromising the rest of the platform.
- Risk-assess each service, including by reference to the factors listed in Section 90(2), to build and strengthen arguments that your service does not permit harmful online activities (if you are ever challenged).

Authors

Tanvi Mehta Krensel
Partner, Sydney
T + 61 450 657 742
E tanvi.mehtakrensel@squirepb.com

Richard Shaw
Law Graduate
T +61 8 9429 7403
E richard.shaw@squirepb.com