ONLINE SAFETY (RELIEF AND ACCOUNTABILITY) ACT 2025 – PROMOTING ACCOUNTABILITY AND EMPOWERING

CONTENTS

Introduction

The Online Safety (Relief and Accountability) Bill was passed in Parliament on 5 November 2025 and received the President's assent on 25 November 2025. Although as of the date of this article, the Online Safety (Relief and Accountability) Act 2025 ("**Act**") has yet to come into effect, its passage marks a significant new phase in Singapore's online safety regulatory landscape.

(a) Part 1 of this article will discuss the key rights and obligations introduced by the Act, including the expanded scope of online harms recognised, and the channels through which victims of online harm can seek and secure timely redress.

(b) In Part 2 of this article, we will take a step back and explore how the Act fits into the wider regulatory landscape in Singapore, and what other protections already exist.

(c) Finally, Part 3 of this article will discuss how the protections and obligations introduced by the Act may affect businesses and victims moving forward.

Part 1: Key Rights and Obligations

In a nutshell, the Act introduces two significant developments that would benefit victims of online harms:

(a) Statutory torts have been created vis-à-vis certain categories of online harmful activities, giving individuals greater clarity and certainty over the remedies that they are able to seek against perpetrators of online harms. Statutory duties and torts have also been created for intermediaries such as online service providers, who are recognised as having the capability to prevent, detect, and respond to online harms on the online platforms they operate. This helps to alleviate the burden of self-protection away from individual users.

(b) The Act allows for victims of online harm to seek timely relief without having to undergo lengthy court proceedings, through the newly created role of the Commissioner of Online Safety / Online Safety Commission ("**OSC**"). The OSC is anticipated to be set up in the first half of 2026[1] and will be empowered to issue directions to entities such as perpetrators of online harms, content administrators and social media platforms, in response to online harm reports received.

On the other hand, digital intermediaries such as online service providers will likely require a review of internal policies and processes to manage the following notable developments:

(a) Potential tortious liability may arise under statutory torts, such as failing to respond reasonably to assess and address online harms that have been reported in respect of their platforms.

(b) Various directions and orders may be issued against online service providers, and it will be a criminal offence to fail to comply. For instance, the OSC will be empowered to issue content takedown directions, or orders requesting for information and documents from social media platforms to identify perpetrators of online harm. These online service providers will be required to support relief mechanisms under the Act and comply with heightened regulatory expectations to assist victims of online harms.

[1] https://www.gov.sg/explainers/parliament-nov2025/

What online harms are covered and what are the new statutory torts?

The Act is intended to cover 13 types of technology-neutral online harmful activities. However, the OSC's focus will initially be on addressing the most prevalent and severe online harms, these being online harassment (including sexual harassment), intimate image abuse, image-based child abuse, doxxing and online stalking.[2]

Several of the online harmful activities will be classified as statutory torts, and victims will be able to bring civil proceedings in court against perpetrators of such statutory torts. Notably, not all the online harms will be classified as statutory torts to avoid overlap and double remedy with existing laws. There are also certain harms that are deemed unsuitable to be dealt with in a litigious setting (i.e., incitement of enmity).[3]
The Act has also been future-proofed as it allows for the Minister for Digital Development and Information to prescribe additional types of online activity that are likely to cause harm to persons in Singapore.[4]

An overview of the online harmful activities set out in the Act and their status as statutory torts is set out below.

S/N	Type of Online Harm	Description	Statutory Tort Status
1.	Online harassment	Communication of online material that a reasonable person would conclude is threatening, abusive, insulting, sexual or indecent, and likely to cause a person harassment, alarm, distress or humiliation.	Yes, to the extent that the tort applies to "Administrators" and "Online Service Providers" facilitating / permitting the activity or failing to respond reasonably to an online harm notice, as the case may be. "Communicators" of the relevant material will continue to be dealt with under the Protection from Harassment Act 2014 to prevent overlap.
2.	Doxxing	The publication of any identity information of a person that a reasonable person would conclude was likely to have been intended to cause harassment, alarm, distress or humiliation.	
3.	Online stalking	A course of online conduct engaged in by the online stalker that involves online acts or omissions associated with stalking, and that a reasonable person would conclude is likely to cause the victim harassment, alarm, distress or humiliation.	
4.	Non-consensual disclosure of private information	Publication of private information without the victim's consent and that a reasonable person would conclude is likely to cause the victim harassment, alarm, distress or humiliation.	No, overlaps with privacy and confidentiality laws.

[2] https://www.gov.sg/explainers/parliament-nov2025/. See also https://www.mlaw.gov.sg/files/Annex___Proposed_New_Law_to_Empower_Victims_of_Online_Harms_to_Seek_Timely_Relief_and_Obtain_Redress.pdf
[3] https://www.mlaw.gov.sg/second-reading-speech-of-the-online-safety-relief-and-accountability-bill-2025-by-minister-of-law-edwin-tong/
[4] https://www.mddi.gov.sg/newsroom/second-reading-closing-speech-by-mos-rahayu-mahzam-on-the-online-safety--relief-and-accountability--bill/

5.	Publication of false material	Publication of online material that contains or consists of a false statement of fact about the victim that a reasonable person would conclude is likely to cause harm to the victim.	No, overlaps with law of defamation.
6.	Publication of statement harmful to reputation	Publication of online material that contains or consists of a statement that a reasonable person would conclude is likely to cause the victim harm to their reputation and any other additional harm.	
7.	Incitement of enmity	Communication of online material that a reasonable person would conclude incites, or is likely to incite, feelings of enmity, hatred or hostility against any group in Singapore.	No, inappropriate to be dealt with by the courts, to be dealt with by the OSC instead.
8.	Incitement of violence	Communication of online material that a reasonable person would conclude incites or is likely to incite one or more persons to use unlawful force or unlawful violence against any group in Singapore.	Yes
9.	Online instigation of disproportionate harm	Communication of online material that tends to instigate the public to act or omit to act in response to an alleged speech or conduct of a victim or their associate in a manner which increases the risk of the victim suffering harm, and where such harm is disproportionate to the wrongfulness (if any) of the alleged speech or conduct, or of any relevant actual speech or conduct of the victim or their associate.	Yes, but this tort only applies to "Communicators".
10.	Intimate image abuse	Communication of online material that non-consensually contains an intimate image or recording of the victim, an offer to sell or distribute an intimate image or recording of the victim; and that a reasonable person would conclude is likely to cause the victim harassment, alarm, distress or humiliation.	Yes
11.	Image-based child abuse	Communication of online material that contains a child abuse image or recording of a victim, an offer to sell or distribute a child abuse image or recording of the victim, an advertisement of a child abuse image	Yes

		or recording of the victim, or any material which appears to be designed or communicated in such a way as to lead to any child abuse image or recording of the victim.	
12.	Online impersonation	Online activity conducted which involves pretending to be the victim without the victim's consent and would lead a reasonable person to believe that the online activity was conducted by the victim when this was not in fact the case.	Yes
13.	Inauthentic material abuse	Communication of inauthentic material of a victim that a reasonable person would conclude is likely to cause the victim harassment, alarm, distress or humiliation because it is false or misleading. This includes false or misleading material that has been altered or generated that is realistic enough for a reasonable person to believe that the victim said such words or engaged in such actions or conduct, such as images or videos generated using deepfake AI technology.	Yes

Statutory torts have also been created vis-à-vis perpetrators as well as intermediaries, these being entities that are not the perpetrators but are in a position to facilitate the online harm and/or address the harm. The Act sets out duties and torts that apply to those classified as "Communicators", "Administrators" and "Online Service Providers".[5]

(a) Communicators:
- These are perpetrators of the online harmful activities. They have a statutory duty not to communicate, publish, and/or engage in any conduct relating to any specified online harm in Singapore.

(b) Administrators:
- These are usually persons that operate and moderate online platforms and may have varying powers and control over the platform. They have been defined broadly in the Act as persons who may "*develop and maintain the online location*", "*organise, manage or supervise the use of the online location*", "*manage or regulate membership of, or access to, the online location*" or have the "*authority to decide whether any material may be included on or excluded from the online location or where to place the material on the online location, or otherwise exercise editorial control over the online location*".

[5]The duties and torts applicable to administrators and online service providers only apply to the following online harmful activities: online harassment, doxxing, online stalking, intimate image abuse, image-based child abuse, online impersonation, inauthentic material abuse, and incitement of violence.

- They have a statutory duty not to develop or maintain an online location in a manner that facilitates or permits online harm to take place – with the intention or knowledge that online harm is likely to take place. This duty is to cover Administrators who may be complicit in the online harms committed.
- When notified of harm, they also have a duty to take reasonable care to assess if there is harm and if so, to take reasonable steps to address it.

(c) Online Service Providers:
- These are typically social media platforms, and the definition in the Act excludes providers of internet access services and app distribution services.
- Similar to administrators, when notified of harm, online service providers must take reasonable care to assess if there is harm and if so, to take reasonable steps to address it.
- Conversely, it is also a tort to send frivolous or false online harm notices to online service providers.

What powers does the OSC have?

Directions

The OSC will be empowered to issue directions to address the 13 aforementioned categories of online harms. Upon receiving a report, the Commissioner may give one or more directions to either the Communicator, Administrator, or Online Service Provider, depending on what may be appropriate in the circumstances.

The Act prescribes a wide range of directions, and there are specific recipients for each type of direction. For instance, an access disabling direction may only be given to an online service provider, and a labelling direction may only be given to an administrator of the relevant location.

Non-compliance with such directions issued by the OSC will be classified as a criminal offence, and the OSC is empowered to make orders such as access blocking of content, or app removal.

End-user identification measures

Perpetrators of online harm are emboldened by the ability to remain anonymous. This ability, among other things, may inhibit their victims from obtaining legal recourse as proceedings cannot be commenced, and Court judgments cannot be enforced, against unknown persons.

Parliament has recognised that pre-existing legal mechanisms for identifying the defendant may be too costly and time-consuming for most individuals and may hinder their efforts to seek redress. In this regard, the Act proposes end-user identification measures and powers for the OSC such as:

(a) The ability to require an Online Service Provider to retain all relevant records in relation to an alleged online harmful activity that has been committed, or any end user who has been reasonably suspected of engaging in an online harmful activity.

(b) The ability to obtain information and documents for the discharge of its functions. For instance, where the OSC reasonably suspects a user of committing an online harm, and the information that the OSC requires is contained in a computer or electronic device, the OSC may require any person to provide assistance in gaining access to that computer or device, by providing the username, password or other authentication information in their possession.

(c) The ability to require an Online Service Provider to take reasonable steps to obtain specified information of an end-user that may identify or lead to the identification of that end-user (whether that end-user is in Singapore or outside Singapore) and provide that information to the OSC.

(d) The ability to disclose the perpetrator's identity information or contact details to a victim or to their authorised representatives, upon receiving an application from the victim. Although the OSC, in approving such a request, may impose conditions such as restraining the applicant from publishing the information or using the information for any purpose other than the purpose for which the application was approved.

What remedies are available?

Once a victim successfully establishes a claim, the Court may award damages that it thinks to be just and equitable in the circumstances. The Court may also make an award for damages such as compensation for loss of earnings or an account of profits where perpetrators have benefitted from the harm.

Given the nature of online harms, certain losses may not be easily established and quantified, especially for non-economic losses like damages for emotional distress. Ultimately, it will be for the victim to prove their loss and for the Court to award a fair remedy based on the facts of each case. In certain cases where the online harm may be imminent, the Court will be empowered to issue injunctions, which operate independently of directions from the OSC and would offer victims an additional, complementary route to obtaining relief.

The Court is also empowered to award enhanced damages in addition to any general and special damages that may be awarded if it thinks just and equitable, but only in respect of proceedings brought by a victim of a statutory tort committed by a Communicator under Part 10 of the Act, and in the case of Administrators, the tort of facilitating or permitting an applicable online harmful activity.

Enhanced damages may be awarded where the victim had made a reasonable request to the Communicator or Administrator to address the online harmful activity, but they had failed without reasonable excuse to address it within a reasonable time. Such enhanced damages are intended to target those who are the root cause of the harm, such as recalcitrant Communicators or Administrators who have encouraged such harms by creating harmful websites and chat groups.[6]

Part 2: Interaction with other Online Safety Laws

Aside from introducing the new statutory obligations and remedies above, the Act is intended to complement and improve the efficacy of existing laws. In particular, significant amendments have been proposed in the Act pertaining to the Protection from Harassment Act 2014 ("**POHA**"). Notable changes include:

(a) An updated definition of offences causing "harassment, alarm or distress" to include causing "humiliation". The description of such offences has also been updated to incorporate conduct that involves "sexual or indecent" words, behaviour, and/or communication. This is in line with the definition of online harmful activities in the Act, where activities such as online harassment, doxxing, and intimate image abuse are recognised as being able to cause the victim humiliation.

(b) The Court will be empowered to award enhanced damages for POHA offences if it thinks just and equitable to do so in the circumstances. This will help to ensure that victims receive proper

[6] https://www.mlaw.gov.sg/second-reading-speech-of-the-online-safety-relief-and-accountability-bill-2025-by-minister-of-law-edwin-tong/

compensation, taking into account the nature of the online harm caused in each case. This is also in line with awarding enhanced damages under the Act, which has been discussed above.

(c) In alignment with the Act, the concept of "Administrators" will also be introduced in POHA, and appropriate directions may be issued by the Court against Administrators, such as a "stop publication (administrator) order" and a "correction (administrator) order".

Once the Act comes into force, it will operate in tandem with the broader suite of Singapore's online safety laws, enhancing the remedies available to victims. For example, in the case of publication of a statement that is harmful to one's reputation, the Act provides an alternative and/or concurrent remedy to a defamation suit, which is a Right-of-reply Direction issued to allow the victim to issue their reply quickly to minimise harm done to their reputation, which matters due to the speed at which allegations may spread.

The suite of online safety laws also seeks to regulate and strengthen the practices of intermediaries in order to foster a safer online environment. Beyond their statutory obligations to respond to reports of online harm and to comply with directions issued by the OSC, intermediaries may also be subject to additional responsibilities under the applicable Codes of Practice, depending on their role in the digital ecosystem, e.g., whether they are a social media service provider, e-commerce platform, or app distribution service provider.

The diagram below provides a brief overview of how key online harms may be addressed by the various online safety laws and regulations in Singapore.

Harassment, doxxing, stalking	• Victims may apply for court-ordered protection against the perpetrators under the **Protection from Harassment Act 2014**. • Where relevant, victims may also report Administrators and Online Service Providers to the OSC under the **Online Safety (Relief and Accountability) Act 2025** for facilitating / permitting the harassment, doxxing or stalking, or failing to respond reasonably to an online harm notice, as the case may be.
Scams, fraud, malicious cyber activities under the Computer Misuse Act 1993, and other specified offences	• The Singapore Police Force have powers under the **Online Criminal Harms Act 2023 (OCHA)** to prevent and disrupt scams, fraud, and malicious cyber activities. In this regard, they may order takedowns of illegal or exploitative material across platforms. • The **Code of Practice for E-Commerce Services and Code of Practice for Online Communication Services** (issued pursuant to OCHA) requires e-commerce platform services and online communication services to take measures to protect users from scams.
Falsehoods, misinformation, or defamatory material	• Users may rely on correction directions issued under the **Protection from Online Falsehoods and Manipulation Act 2019 (POFMA)** to access verified information. POFMA targets both individuals and internet intermediary services. • Publication of false material and/or statements harmful to reputation (that do not need to be true), are online harmful activities that may be reported to the OSC under the **Online Safety (Relief and Accountability) Act 2025**. • Defamatory statements may be prosecuted under Section 499 of the **Penal Code 1871**. Civil claim may also be brought under the **Defamation Act 1957** (including unintentional defamation).
Sexual, violent, suicide, self-harm, cyberbullying content	• The **Code of Practice for Online Safety – Social Media Services (the "Social Media Services Code")** and **Code of Practice for Online Safety for App Distribution Services (the "App Distribution Services Code")** (issued pursuant to the Broadcasting Act 1994) target designated social media services and app distribution services, requiring them to implement measures to curb the spread of harmful and inappropriate content on their platforms and protect vulnerable child users by implementing content safety and parental controls. • The **Online Safety (Miscellaneous Amendments) Act 2022**, among other things, amends the Broadcasting Act 1994 to empower IMDA to issue codes of practice and directions to online communication services and internet access service providers to disable / block harmful and inappropriate content.
Non-consensual disclosure of private information, intimate image abuse, image-based child abuse	• These are online harmful activities that may be reported to the OSC under the **Online Safety (Relief and Accountability) Act 2025**. • Further, the **Criminal Law (Miscellaneous Amendments) Bill** was passed in Parliament on 4 November 2025. When in effect, it will enhance penalties under existing criminal laws, including harms that may be perpetuated online such as circulation of obscene materials, including child abuse materials, and doxxing. Laws will also be updated to get ahead of technological developments, such as producing “deep fakes” without making use of a pre-existing image or recording.

Part 3: Guidance for Business and Victims

What businesses should note

Compliance with the obligations introduced under the Act will inevitably entail additional operational and financial costs. Prior to the Act coming into effect, affected organisations may wish to start taking the following preparatory steps for compliance:

- **Conduct initial gap assessments against the regulatory thresholds and requirements in Singapore for purposes of updating existing policies and procedures:** These assessments may cover not only compliance with the Act, but also other relatively recent requirements such as the Social Media Services Code (in the case of designated Social Media Services) and the App Distribution Services Code (in the case of designated App Distribution Services). The gap assessment may cover broad categories such as content governance, risk controls, and inter-departmental escalation protocols.

  Crucially, organisations should ensure that there are policies and procedures to identify and deal with the 13 categories of online harmful activities covered under the Act. Given that the OSC is also empowered to require organisations to provide end-user identity information, organisations may need to beef up their user verification, record retrieval and data retention policies and ensure that their platform terms of use adequately obtain consent and notify such purposes of disclosure (although we note that it is also possible for such disclosure to otherwise fall under a relevant exception to consent in the PDPA).

- **Implement response protocols:** Dedicated teams and protocols may need to be put in place to comply with the directions (within the prescribed timeframes) that may be issued by the OSC in Singapore that are not otherwise required in other markets that the business operates in. Organisations also need to have in place procedures to manage and respond to online harm notices, while existing procedures for responding to takedown or content moderation directions (for example, in accordance with directions issued under OCHA) will likely require review and refinement.

Nevertheless, we note that the Act does not require online service providers or administrators to proactively scan for harms. Instead, their duty is to act responsibly once notified. Nor are they expected to respond to every single online harm notice that has been submitted. To prevent online service providers and administrators from being inundated with frivolous or incomplete filings, an online harm notice must include prescribed particulars in a specified form. This ensures that the necessary categories of information are provided upfront, so that only genuine, properly documented cases trigger the duty to act. [7]

Aligning internal policies with the new regime also presents an opportunity for online service providers to strengthen governance. Swift, effective compliance will allow online service providers to demonstrate a clear commitment to user safety, while transparent cooperation with authorities can help restore consumer trust – particularly among users who have experienced harms facilitated through online platforms, as well as users who have grown more cautious and sceptical in the current digital environment.

[7] https://www.mlaw.gov.sg/second-reading-speech-of-the-online-safety-relief-and-accountability-bill-2025-by-minister-of-law-edwin-tong/

What victims should note

The protections introduced under the Act add another layer to the existing rights and remedies available to victims.

That said, victims will generally need to first report the harm they have experienced to the relevant online service provider before escalating the matter to the OSC. Although for specific categories of online harm that warrant urgent intervention and relief, such as intimate image abuse and image-based child abuse, victims will be allowed to seek immediate redress from the OSC.[8]

At first glance, the range of options available under the suite of legislation relating to online safety may seem overwhelming, and victims may now be uncertain about the most appropriate avenue for relief. To address this, the OSC is expected to operate a "no wrong door" policy to guide victims towards the appropriate agency for the assistance they require. In practice, this will be supported by inter-agency coordination to streamline processes and minimise the need for victims to make multiple reports.[9]

Conclusion

Parliament clearly recognises that individuals, acting alone, cannot reasonably be expected to fend off increasingly sophisticated harms perpetrated by malicious actors emboldened by online anonymity. Recognising that online harms may unfold and escalate rapidly, the protections in the Act prioritise and underscore the importance of timely intervention.[10]

The Act's intent appears to be establishing a model of shared responsibility among online service providers, administrators, and victims. Providers must design platforms with safety as a core principle and maintain operational readiness to prevent and respond to online harms, while users should engage responsibly, understand how to protect themselves, and know how to report harms and seek redress.

---

[8] https://www.mlaw.gov.sg/proposed-new-law-to-empower-victims-of-online-harms-to-seek-timely-relief-and-obtain-redress/. See also https://www.mlaw.gov.sg/files/Annex___Proposed_New_Law_to_Empower_Victims_of_Online_Harms_to_Seek_Timely_Relief_and_Obtain_Redress.pdf.
[9] https://www.mddi.gov.sg/newsroom/second-reading-closing-speech-by-mos-rahayu-mahzam-on-the-online-safety--relief-and-accountability--bill/
[10] https://www.mlaw.gov.sg/second-reading-speech-of-the-online-safety-relief-and-accountability-bill-2025-by-minister-of-law-edwin-tong/

DREW DATA PROTECTION & CYBERSECURITY ACADEMY

Drew Data Protection & Cybersecurity Academy (Drew Academy) was established in 2020 by Drew & Napier to help our clients build their capabilities and develop and implement organisational strategies, structures, policies and processes to meet their legal, regulatory and compliance obligations. Drew Academy offers a range of courses in areas such as data protection, cybersecurity, data governance and in-house commercial practice. A particular focus for us is the delivery of workplace learning solutions and development of customised training courses. We also offer outsourced Data Protection Officer (DPO) services and data protection consulting services through our experienced team of practitioners.

Drew Academy is helmed by Lim Chong Kin and David N. Alfred. Our course leaders are experienced in various aspects of data and cyber governance, data protection, cybersecurity engineering, and in-house commercial practice.

ARTIFICIAL INTELLIGENCE AND DIGITAL TRUST

Drew & Napier's Artificial Intelligence (AI) and Digital Trust practice brings together its expertise across several technology-related domains and in fields as diverse as data protection, cybersecurity, healthcare, Fintech, intellectual property and competition law (to name a few) to advise clients on the full range of legal issues relating to AI and Digital Trust. In addition to advising on commercial, regulatory and international / cross-border issues, our advice extends into areas such as governance and ethics as we seek to enable our clients to navigate areas where laws and legal principles are still emerging.

Working together with the Drew Academy, we provide solutions that reflect our deep understanding of underlying technologies, the risks and uncertainties involved and practical business considerations.
Internationally, there is a growing consensus on AI governance.

For more information on our experience, please contact:

Lim Chong Kin
Managing Director, Corporate & Finance;
Co-Head, Data Protection, Privacy & Cybersecurity Practice;
Co-Head, Drew Data Protection & Cybersecurity Academy

T: +65 6531 4110
E: chongkin.lim@drewnapier.com

Lim Shao Min
Senior Associate, Corporate & Finance

T: +65 6531 4122
E: shaomin.lim@drewnapier.com

DREWACADEMY
DATA PROTECTION & CYBERSECURITY SERVICES

10 Collyer Quay
10th Floor, Ocean Financial Centre
Singapore 049315

www.drewnapier.com/Academy

T: +65 6531 3699
E: academy@drewnapier.com

In association with

DREW & NAPIER