
CHAMBERS GLOBAL PRACTICE GUIDES

Defamation & Reputation Management 2026

Definitive global law guides offering
comparative analysis from top-ranked lawyers

Singapore: Law & Practice and Trends & Developments

Tony Yeo, Kelvin Tan, Gary Low and Meryl Koh
Drew & Napier LLC



SINGAPORE



Law and Practice

Contributed by:

Tony Yeo, Kelvin Tan, Gary Low and Meryl Koh

Drew & Napier LLC

Contents

1. Privacy and Confidentiality p.4

- 1.1 Privacy Grounds p.4
- 1.2 Privacy Remedies p.4
- 1.3 Privacy Deadlines and Defences p.5
- 1.4 Privacy Proceedings Forum Choice p.5
- 1.5 Privacy Costs p.5
- 1.6 Other Features of Privacy Actions p.5

2. Defamation p.6

- 2.1 Defamation Grounds p.6
- 2.2 Defamation Remedies p.6
- 2.3 Defamation Deadlines and Defences p.7
- 2.4 Defamation Proceedings Forum Choice p.8
- 2.5 Defamation Costs p.9
- 2.6 Other Features of Defamation Actions p.9

3. Harassment p.9

- 3.1 Harassment Grounds p.9
- 3.2 Harassment Remedies p.9
- 3.3 Harassment Deadlines and Defences p.10
- 3.4 Harassment Proceedings Forum Choice p.11
- 3.5 Harassment Costs p.11

4. Data Protection p.11

- 4.1 Data Protection Grounds p.11
- 4.2 Data Protection Remedies p.12
- 4.3 Data Protection Deadlines and Exemptions p.13
- 4.4 Data Protection Proceedings Forum Choice p.14
- 4.5 Data Protection Costs p.14

5. Regulatory and Media Environment p.14

- 5.1 Key News Providers p.14
- 5.2 Regulatory Framework p.15
- 5.3 Complaints Process p.15
- 5.4 User-Generated Content p.15
- 5.5 SLAPPs p.16
- 5.6 Preventing Foreign Judgments p.16

Drew & Napier LLC has been providing exceptional legal service and representation to discerning clients since 1889. It is one of the largest law firms in Singapore. Drew & Napier's defamation practice is part of the firm's dispute resolution practice, which is widely recognised as a frontrunner in the industry. The practice is sought out by high-profile individuals and companies, including international corporations,

banks and other financial institutions, for advice and assistance on defamation-related issues. The firm's lawyers are involved in many major and landmark defamation disputes in Singapore and are constantly breaking new ground. They have experience advising and litigating on a broad range of defamation matters, including cross-border disputes and cases involving defamatory material spanning various forums.

Authors



Tony Yeo is the director of Drew & Napier's intellectual property department, and a director in our dispute resolution department. He also heads our healthcare and life sciences practice. Tony is a litigator

with an active court practice who has acted as lead counsel in many complex matters, including numerous high-stakes litigation cases. In a defamation and malicious falsehood case, he successfully obtained a judgement for the highest amount ever recovered in the Singapore Court by a claimant, against an individual who made statements that he knew were false and which were found to be maliciously made.



Kelvin Tan has an active practice in commercial litigation and international arbitration. He leads Drew & Napier's contentious employment practice. He regularly assists corporate and executive clients protect their industry

and professional reputations, both in litigation and in helping them form strategic approaches to safeguard against reputational damage via traditional and modern media and communications channels. Kelvin also helps clients with reputational concerns in various other areas, including shareholder and fiduciary duty disputes, fraud, false advertising, passing off and impersonation.



Gary Low is involved in all areas of civil, commercial and criminal litigation and is co-head of Drew & Napier's criminal law practice group. He has acted in a wide variety of matters, including defamation claims

and various banking, corporate and contractual disputes. He has also represented clients accused of diverse offences, including commercial crimes, corruption, money-laundering and securities offences, in addition to leading allegations into fraud, criminal breach of trust, breach of fiduciary duty, workplace harassment and other forms of misconduct.



Meryl Koh is a leading commercial litigator in Singapore, widely respected by peers for her expertise in complex civil and commercial disputes. She regularly advises high net worth individuals, public figures

and household brands across the technology, video games, entertainment, sports and media industries. Her practice covers shareholder disputes, intellectual property matters, licensing conflicts, breaches of confidentiality, harassment claims and defamation actions. Meryl was part of the team that secured Singapore's highest damages award for malicious falsehood and defamation. She also successfully represented a YouTube personality with 26 million followers in a defamation suit against a media company and content creator.

Drew & Napier

10 Collyer Quay
10th Floor Ocean Financial Centre
Singapore 049315

Tel: +65 6535 0733
Fax: +65 6535 4906
Email: mail@drewnapier.com
Web: www.drewnapier.com



1. Privacy and Confidentiality

1.1 Privacy Grounds

The two main sources of law are the Personal Data Protection Act 2012 (“PDPA”) and the common law tort for breach of confidence.

PDPA

One of the key requirements under the PDPA is consent. Section 13 of the PDPA provides that organisations must not collect, use or disclose personal data about an individual, unless:

- the individual has given (or is deemed to have given) consent to the collection, use or disclosure; and
- the collection, use or disclosure without the individual’s consent is required or authorised under the PDPA or any other written law.

Pursuant to section 48O of the PDPA, any person who suffers loss or damage directly as a result of a contravention, by an organisation, of any provision of Parts 4, 5, 6, 6A or 6B of the PDPA (which includes the aforementioned section 13) has a right to bring an action for relief in civil proceedings. The Singapore Court of Appeal (“SGCA”) has recognised that emotional distress may be considered a form of loss or damage within the meaning of section 48O of the PDPA.

(See *Reed, Michael v Bellingham, Alex (Attorney-General, intervener)* [2022] SGCA 60 at [68]).

Breach of Confidence

In a claim for breach of confidence, the court must first consider whether:

- the information in question has the necessary quality of confidence about it; and
- the information has been imparted in circumstances importing an obligation of confidence.

If these prerequisites are satisfied, an action for breach of confidence is presumed, and the burden shifts to the defendant to show that their conscience was unaffected.

(See the SGCA in *I-Admin (Singapore) Pte Ltd v Hong Ying Ting and others* [2020] SGCA 32 at [61].)

1.2 Privacy Remedies

For a private civil action under the PDPA, the remedies that may be granted include: injunctions, declarations, damages and/or any other relief the court thinks fit. This is set out in section 48O(3) of the PDPA.

For an action for breach of confidence, the remedies that may be granted include: injunctions, delivery up, destruction and/or damages.

It may be possible to apply for a quia timet or precautionary injunction to restrain a threatened breach. The inquiry has two stages:

- first, the question is whether there is a strong probability that, unless restrained by the injunction, the defendant will act in breach of the claimant’s rights; and

- if the first question is answered in the affirmative, then the second question is whether the harm resulting from the breach would be so grave and irreparable that, notwithstanding the grant of an immediate interlocutory injunction at the time of actual infringement of the claimant's rights, in order to restrain further occurrence of the acts complained of, a remedy of damages would be inadequate.

(See *Gazelle Ventures Pte Ltd v Lim Yong Sim and others* [2023] SGHC 328 at [24].)

The quantum of damages to be ordered depends heavily on the particular facts of each case and the ability of the parties to prove their losses; there is no “normal range” per se.

1.3 Privacy Deadlines and Defences

For claims in tort (which would include a claim for breach of confidence), the limitation period is six years from the date on which the cause of action accrued.

When facing a claim for breach of the PDPA, a defendant may try to demonstrate that relevant exceptions under the PDPA apply. For example, Section 17, read with the First Schedule of the PDPA, provides various exceptions where the collection, use or disclosure of personal data may be done without consent, such as where it is in the national interest, or where it is done by a news organisation solely for its news activity.

When facing a claim for breach of confidence, a defendant may seek to show that one or more elements of the claim have not been established (eg, the alleged confidential nature of documents). The Singapore courts have also recognised that a public interest defence may apply in certain circumstances, where the court is required to balance competing public interests in maintaining confidentiality and ensuring that wrongdoing is not concealed.

However, even if there is a public interest in favour of disclosure, this does not mean that widespread disclosure is permissible. Any disclosure should generally be limited to those who have a proper interest in receiving the information. Ultimately, much will depend on the specific facts of each case.

(See *X Pte Ltd and another v CDE* [1992] 2 SLR(R) 575 at [39]–[42].)

1.4 Privacy Proceedings Forum Choice

The PDPA sets out various criminal offences. For example, section 48D of the PDPA provides that if an individual discloses personal data belonging to an organisation or public agency to another person, where said disclosure is not authorised by the organisation or public agency, and the individual does so:

- knowing that the disclosure is not authorised; or
- in a manner that is reckless as to whether the disclosure is or is not authorised.

The individual will be guilty of an offence. If convicted, the individual will be liable to a fine not exceeding SGD5 thousand, to imprisonment for a term not exceeding two years, or to both.

In general, trials must be heard in open court. However, the court may direct any matter to be heard in private with attendance limited to the parties, their legal representatives and any other person the court allows, should it be in the interests of justice. Examples include where there is highly confidential information involved and/or where vulnerable witnesses are giving testimony.

In general, jurisdiction is established by personal service of originating process on the defendant within Singapore. Alternatively, jurisdiction may be established by substituted service and/or service of originating process on the defendant outside of Singapore, subject to the court's approval.

1.5 Privacy Costs

A successful claimant or defendant will generally be able to recover a portion of their legal costs incurred in pursuing or defending the claim (as the case may be). However, costs are ultimately at the discretion of the court, and the court may choose to depart from this general rule depending on specific circumstances.

1.6 Other Features of Privacy Actions

There are no other unusual features of privacy claims in Singapore.

2. Defamation

2.1 Defamation Grounds

In Singapore, common law principles of the tort of defamation and the Defamation Act 1957 (“Defamation Act”) apply. The two types of defamatory statements are libel and slander. In simple terms, libel is written and slander is oral.

The elements of defamation are that the impugned words must:

- have a defamatory meaning;
- refer to the claimant; and
- be published to a third-party.

Proof of each element is required on a balance of probabilities, and the same elements apply to libel and slander.

Defamatory Meaning

A statement has a defamatory meaning if it:

- tends to lower the claimant in the esteem of right-thinking members of society generally;
- causes the claimant to be shunned or avoided; or
- exposes the claimant to hatred, contempt or ridicule.

(see *Lee Hsien Loong v Review Publishing Co Ltd* [2009] 1 SLR(R) 177 (“*Review Publishing (HC)*”) at [47])

Words can be considered defamatory in their natural and ordinary meaning, and/or in their innuendo meaning. The “natural and ordinary” meaning refers to the literal, implied, inferred or indirect meaning of the words (see *Review Publishing Co Ltd v Lee Hsien Loong* [2010] 1 SLR 52 (“*Review Publishing (CA)*”) at [28]–[29]). An innuendo meaning refers to a meaning, which though not defamatory from the viewpoint of the ordinary reasonable person, is nonetheless defamatory from the viewpoint of people with knowledge of the special meaning of the offending words or the relevant extrinsic facts (see *Review Publishing (CA)* at [26]).

Reference to the Claimant

The claimant must prove that the defamatory words refer to them. This is an objective test of whether a ordinary reasonable person, aware of the relevant circumstances or special facts (if any), would reasonably understand the offending words to refer to the claimant (see *Review Publishing (CA)* at [48]–[49]).

Publication to a Third Party

The claimant must prove that the defendant has “conveyed or communicated the [defamatory words] to at least one other person who has received it” (see *Qingdao Bohai Construction Group Co, Ltd v Goh Teck Beng* [2016] 4 SLR 977 at [35]).

Proof of Special Damage

Libel is actionable per se without proof of special damage.

Special damage refers to “loss capable of estimation in money’s worth” (see *Low Tuck Kwong v Sukanto Sia* [2014] 1 SLR 639 (“*Low Tuck Kwong*”) at [94]) that is “referable to the damage to reputation” (see *Low Tuck Kwong* at [96]).

By contrast, slander generally requires proof of special damage. There are certain exceptions, including, but not limited to, the following categories:

- where the words impute the commission of a crime;
- where the words impute to the claimant a contagious or infectious disease;
- where the words impugn the chastity of, or impute adultery to, any woman or girl (see section 4 of the Defamation Act); or
- where the words are calculated to disparage the claimant in any office, profession, calling, trade or business carried on by him or her at the time of the slander (see section 5 of the Defamation Act).

2.2 Defamation Remedies

The typical remedy for defamation is damages. It is also possible to obtain interim or final injunctions for defamation.

General Damages

Damages are compensatory in nature. A non-exhaustive list of factors which the court will take into account in awarding compensatory damages are (see *Shanmugam Kasiviswanathan v Lee Hsien Yang* [2024] 5 SLR 194 (“KSv LHY”) at [28]):

- the nature and gravity of the defamation;
- the conduct, position and standing of the claimant and the defendant;
- the mode and extent of the publication;
- the natural indignation of the court at the injury caused to the claimant;
- the conduct of the defendant;
- the failure to apologise and retract the defamatory statement;
- the presence of malice; and
- the intended deterrent effect of the damages.

Aggravated Damages

Aggravated damages are a component of general damages and are also compensatory. They are awarded when “the defendant’s conduct before and during trial has aggravated the hurt to the claimant’s feelings”. (see *KS v LHY* at [29]).

A corporate entity is not entitled to aggravated damages because aggravated damages are only awarded for injury to feelings, and companies cannot suffer injury to feelings (see *On Site Car Accessories.SG (KEL Services) v Tang Mun Wah Jerry* [2023] 4 SLR 592 at [37]).

Exemplary Damages

Exemplary damages are not compensatory but punitive. Exemplary or punitive damages will only be awarded “where compensatory damages, after taking account all the circumstances of aggravation, remain an insufficient punishment”. (see *Golden Season Pte Ltd v Kairos Singapore Holdings Pte Ltd* [2015] 2 SLR 751 at [146]).

Injunctions

The court can grant a final injunction restraining publication of any repeated or similar defamatory words, if the defendant has shown a propensity to repeat the defamatory allegation (see *Lee Hsien Loong v Roy Ngerng Yi Ling* [2014] SGHC 230 at [58]).

A court may also grant interim injunctions in circumstances where it is clear that the statement complained of was defamatory, no defence could possibly apply, special circumstances exist in the case to warrant the issue of such exceptional relief (see *Chin Bay Ching v Merchant Ventures Pte Ltd* [2005] 3 SLR(R) 142 (“*Chin Bay Ching*”) at [37]) and there is evidence of a threat or intention to repeat the defamatory imputations (see *Chin Bay Ching* at [43] – [44]).

A quia timet or precautionary injunction could theoretically allow the court to grant injunction to restrain publication of a defamatory statement before it happens, though there are no reported cases dealing with this issue.

2.3 Defamation Deadlines and Defences

Limitation Periods

The limitation period for defamation is six years from the date of the publication of the defamatory content (see section 6 (1)(a) of the Limitation Act 1959 (“Limitation Act”).

Defences

After a claimant establishes the elements of the tort of defamation (see Question 2.1 above), the defendant can avoid liability by proving on a balance of probabilities that a defence applies. The typical defences against defamation charges are:

- justification;
- fair comment;
- qualified or absolute privilege.

Justification

Justification is an absolute defence. The defendant has to prove that the substance or gist of the offending words is true (see *Review Publishing v LHL* at [134]).

Fair Comment

To succeed in the defence of fair comment, the defendant must prove that (see *Review Publishing v LHL* at [139]):

- the words complained of are fair comment;
- the comment is on a matter of public interest;
- the comment is based on true facts; and

- the comment is one a fair-minded person can honestly make on the facts proved.

The defence of fair comment can be defeated by proof of malice on the defendant's part. Malice is found where the defendant did not honestly believe the truth of the comment expressed (see *Soh Rui Yong v Singapore Athletic Association* [2020] SGHCR 7 ("*Soh Rui Yong*") at [18 (b)]).

Qualified Privilege and Absolute Privilege

The defendant can also avoid liability by proving that the defamatory statement was made on an occasion of privilege. Two types of privilege apply, namely qualified privilege and absolute privilege.

Qualified privilege generally refers to circumstances where the defendant has a duty or interest in communicating information, and the third party receiving the information has a corresponding duty or interest in receiving the information. These include, but are not limited, to (see *Lim Eng Hock Peter v Lin Jian Wei and anor* [2009] 2 SLR(R) 1004 ("*Lim Eng Hock Peter*") at [164]):

- statements made between parties who share a common or mutual interest in the subject matter of the communication;
- statements made in the discharge of a legal, social or moral duty;
- statements made in the protection of one's own self-interest;
- fair and accurate reports of certain proceedings; and
- statements made to repel a libellous charge, so long as the statement is made in good faith and without malice.

The categories of qualified privilege are not closed (see *Sin Heak Hin Pte Ltd v Yuasa Battery Singapore Co Pte Ltd* [1995] 3 SLR(R) 123 at [51]).

Qualified privilege can be defeated by proof of malice on the defendant's part where:

- the defendant knows the statement is false or does not believe in the truth of the statement; or

- where the defendant has a genuine or honest belief in the truth of the statement, but their dominant motive is to injure the defendant, or some other improper motive.

Absolute privilege is a complete defence which cannot be defeated by proof of malice. Absolute privilege applies only in limited situations, including statements made in judicial or quasi-judicial proceedings, parliamentary proceedings and official state proceedings (see *Lim Eng Hock Peter* at [156]). This includes statements by witnesses giving evidence, or by Members of Parliament during parliamentary proceedings.

Absolute privilege also applies to statements made to the police in police reports.

Other Defences

Other defences include those under the Defamation Act, including making an offer of amends (section 7 of the Defamation Act). This applies to innocent publication of defamatory words, where the defendant publishes a correction and apology, among other things.

2.4 Defamation Proceedings Forum Choice Criminal Defamation

Defamation is also a criminal offence under Chapter 21 of the Penal Code 1871 ("Penal Code"). The most significant difference is in the standard of proof because criminal defamation must be proved beyond a reasonable doubt.

The elements of criminal defamation are generally the same as the tort of defamation (ie publication of a false statement, with a defamatory meaning, which refers to the claimant).

In addition, criminal defamation under section 499 of the Penal Code requires that the offender had intended to harm, or knew, or had reason to believe, that his publication would harm the victim's reputation. By comparison, the tort of defamation does not require intent to harm.

Criminal prosecution is within the discretion of the Public Prosecutor, and prosecution of an offence of criminal defamation can only be instituted with the consent of the Public Prosecutor.

Court Proceedings Are Public

Court proceedings in Singapore, including for defamation, are public by default.

All court proceedings, including for defamation, are heard in public, in accordance with section 8 (1) of the Supreme Court of Judicature Act 1969. Although the court has the discretion to have hearings in private, this is rare and would not apply to defamation proceedings.

Natural Forum

A full explanation of conflicts of law is beyond the scope of this Q&A. As a general overview:

- the court will consider the place where the tort happened. For defamation under Singapore law, the place of the tort is where the defamatory material was published. For internet publications, this is ordinarily where it is accessed and downloaded by third-parties (see *Ng Koo Kay Benedict v Zim Integrated Shipping Services Ltd* [2010] 2 SLR 860 at [26]);
- the location of the defendant is not determinative. The Rules of Court 2021 (“ROC 2021”) allow service of defamation claims out of jurisdiction; and
- the location of the claimant is also not determinative, although it will have an impact on where the claimant’s reputation was harmed.

2.5 Defamation Costs

Costs are ordinarily recoverable by the successful party. The general rules applicable to costs in the ROC 2021 also apply to defamation claims.

The amount of costs awarded by the court does not operate as a full indemnity of a party’s incurred legal costs. Instead, the legal costs recoverable from the losing party represent only a portion of that party’s incurred costs.

2.6 Other Features of Defamation Actions

Defamation claims commenced in the State Courts (which includes the Magistrate’s Court and District Court) must comply with the pre-action protocol in Appendix F of the State Courts Practice Directions 2021. The protocol requires the sending of a pre-action letter of claim setting out sufficient details of the

defamation, why the alleged defamatory publication is false, identification of the claimant and any special facts, as well as the remedies sought by the claimant, among other things.

The protocol aims to facilitate pre-action exchange of information, encourage constructive negotiation and improve the chances of pre-action settlement. Non-compliance with the protocol can be taken into account when the court makes costs orders.

There is no similar pre-action protocol for claims commenced in the High Court, although the sending of letters of demand is a common practice. In any event, Rule 5 of the ROC 2021 provides that parties have a duty to consider amicable resolution before commencing proceedings.

3. Harassment

3.1 Harassment Grounds

The common law tort of harassment has been abolished in Singapore and replaced by the Protection from Harassment Act 2014 (“POHA”). All civil claims for harassment must be brought under POHA.

POHA sets out various criminal offences under section 3 (intentionally causing harassment, alarm or distress), section 4 (actions likely to cause harassment, alarm or distress), section 5 (fear, provocation or facilitation of violence), and section 7 (unlawful stalking).

Section 11 allows a victim to commence civil proceedings for contraventions of sections 3, 4, 5 and 7 of POHA.

3.2 Harassment Remedies

Protection Order

The victim of a breach of sections 3, 4, 5, 6 or 7 of POHA can apply for a protection order, which can include orders that:

- prohibit the respondent from doing anything in relation to the victim or related person;
- if the likely or continuing contravention of sections 3, 4, 5, 6 or 7 of POHA involve an offending communication, require the respondent to stop pub-

- lishing the offending communication or anything similar; and/or
- refer the respondent, the victim or a related person to attend counselling or mediation.

Where there is an application for a protection order, the court can also grant an expedited protection order. This is an interim order, based on prima facie evidence that the respondent has breached POHA, where such continued contravention is likely to have a substantial adverse effect on the victim.

Other Remedies

The court may also make various orders in relation to false statements including (section 15 (1) of POHA):

- a stop publication order;
- a correction order;
- a disabling order;
- a targeted correction order; and/or
- a general correction order.

The applicant must prove on a balance of probabilities that the statement is false and has been published by the respondent, among other things. These orders also apply to parties outside Singapore (see section 15 (4) of POHA).

A stop publication order requires the respondent to stop publishing the false statement and to not publish any substantively similar statement.

A correction order requires the respondent to publish a correction notice in a specified manner (whether physically or online), which may include that the statement has been determined by the court to be false, or otherwise correcting the false statement of fact. A targeted correction order is similar to a correction order but applies to an internet intermediary, requiring publication to users in Singapore of the internet intermediary's service.

A disabling order applies to an internet intermediary and requires the internet intermediary to disable access to the false statement by users of the internet intermediary's service in Singapore.

A general correction order is a more specialised remedy. Unlike the other POHA orders, it requires proof that the publication has caused, or is likely to cause, serious harm to the applicant's reputation.

Where the publisher has a newspaper, broadcasting or telecommunications licence, or is a prescribed internet intermediary, the general correction order can require the publisher to publish a general correction notice in a particular media format applicable to that publisher (eg, in the newspaper, by an internet intermediary service), stating that the statement has been determined by the court to be false, or otherwise correcting the false statement of fact.

Damages

Damages can be awarded in civil proceedings for breach of POHA. The damages awarded are the amount the court thinks is "just and equitable" (see section 11 (2) of POHA).

The quantum of damages awarded in POHA claims are often low and may fall in the range of a few thousand Singaporean dollars. The main remedy in POHA claims is the cessation of the offending conduct, rather than award of damages.

3.3 Harassment Deadlines and Defences

Limitation Periods/Deadlines

In general, the limitation period for harassment is six years from the date the cause of action has accrued (see section 6 (1)(a) of the Limitation Act).

Civil claims under POHA can be brought as "Simplified Proceedings" under Part 2 of the Supreme Court of Judicature (Protection from Harassment) Rules 2021 ("POHA Rules") or "Standard Proceedings" under Part 3 of POHA Rules (see Question 3.4 below).

A claim under the simplified proceedings track can only be brought within two years after the cause of action has accrued.

Defences

The available defences depend on the relevant provision of POHA contravened.

For section 3 of POHA, it is a defence if the accused can prove that their conduct was reasonable.

For section 4 and section 5 of POHA, it is a defence for the accused to prove that their actions were reasonable, or that they had no reason to believe how their words or conduct would be perceived by the victim.

For section 6, it is a partial defence if the accused did not know the victim was acting as a public servant. In such a situation, section 6 would not apply, but the other sections of POHA would still apply. The other defences available for offences under section 4 of POHA similarly apply.

For section 7 of POHA, there are numerous possible defences, including proof that the conduct was reasonable. Apart from this, the other defences are exceptions to prevent proper investigative police work falling within the scope of stalking.

3.4 Harassment Proceedings Forum Choice Civil Claims

For civil proceedings, claims are heard by the Protection from Harassment Court. Claimants can commence proceedings under either the “Simplified Proceedings” or “Standard Proceedings” track. The “Simplified Proceedings” track adopts simpler procedural rules, and parties are by default not allowed to be represented by lawyers without the court’s permission. The “Standard Proceedings” track adopts rules similar to those in general civil litigation.

Criminal Prosecution

Harassment under POHA is also a criminal offence.

The main distinction is the standard of proof. A criminal offence of harassment requires proof beyond a reasonable doubt, and a civil claim for harassment requires proof on a balance of probabilities. The elements are otherwise the same, under sections 3 to 7 of POHA.

Court proceedings under the “Standard Proceedings” track are public.

For civil proceedings under the “Standard Proceedings” track, please refer to Question 2.4 above.

Court proceedings under the “Simplified Proceedings” track are usually private.

For civil proceedings under the “Simplified Proceedings” track, they will generally be conducted in private unless otherwise ordered by the court (see rule 28 (1) of the POHA Rules).

3.5 Harassment Costs

Costs for simplified proceedings are lower compared to standard proceedings.

In simplified proceedings, the parties are ordinarily self-represented and can only be represented by solicitors with the court’s permission. Although costs are at the court’s discretion, this is subject to the principle that litigants must not profit from the costs of legal proceedings. Compensation for the time of self-represented litigants is therefore ordinarily less than the amount awarded for the costs of legal representation (see *Mah Kiat Seng v Attorney-General* [2024] 5 SLR 1206 at [27]).

For standard proceedings, although the POHA Court is a district court, the scale of costs applied is the scale applicable to the Magistrate’s Court (see rule 61 (1) of the POHA Rules). This means that the costs awarded to the successful party will be lower.

4. Data Protection

4.1 Data Protection Grounds

Singapore’s data protection framework is primarily governed by the Personal Data Protection Act (“PDPA”). The PDPA was recently comprehensively amended, with most provisions taking effect from 1 February 2021. These amendments introduced key legal and/or regulatory grounds for protecting data rights, such as mandatory breach notification, enhanced individual rights and criminal liability for egregious misuse.

Pursuant to section 13 of the PDPA, the starting point for processing personal data under the PDPA is consent. Organisations must notify individuals of the purposes for which their personal data will be collected, either before, or at the point of, collection, and

valid consent must be obtained. Consent need not always be express. For example, in accordance with section 15 of the PDPA, an individual is deemed to have consented where they voluntarily provide their personal data to an organisation for a purpose and it is reasonable that they would do so. Consent may be withdrawn at any time upon reasonable notice (see section 16 of the PDPA).

Beyond consent, the PDPA recognises several statutory exceptions permitting collection, use or disclosure without consent under section 17, read with the First or Second Schedule of the PDPA. These include:

- where processing is necessary for the legitimate interests of the organisation or a third party, such as for the provision of legal services or any other legal proceedings, provided these are not outweighed by the individual's interests;
- for research, historical, or statistical purposes;
- for business improvement purposes; and
- in employment-related contexts, such as managing or terminating an employment relationship.

Organisations are generally bound by eleven core obligations under the PDPA, namely: accountability, notification, consent, purpose limitation, accuracy, retention limitation, protection, transfer limitation, access and correction, data breach notification, and data portability. These are set out under Parts 4, 5, 6, 6A and 6B of the PDPA.

The PDPA is complemented by sector-specific frameworks. For example, the healthcare sector is governed by additional requirements under the Ministry of Health's regulatory framework. Telecommunications data is subject to the Telecommunications Act, which is administered by the Infocomm Media Development Authority ("IMDA").

The PDPA expressly excludes public agencies. Government bodies are not bound by the PDPA and/or the regulatory oversight of the PDPC but are instead subject to the Public Sector Governance Act 2018 ("PS(G)A") and internal government instruction manuals. The distinction is deliberate, as unlike the private sector, the Government is expected to deliver services

in an integrated manner across agencies, and data protection measures will differ accordingly.

Members of the public can make reports of any unauthorised disclosure or compromise of personal data, or raise any concerns about how personal data is used, through the agency's Quality Service Manager, or the Government Data Incident Reporting Platform.

If the data contains confidential information about an individual (eg, medical history, salary information), it might be protected under the tort of breach of confidence, which was mentioned at 1.1 above. This requires the plaintiff to show that the information in question has the necessary quality of confidence about it, and that the information has been imparted in circumstances importing an obligation of confidence. This tort might be more relevant for situations where the PDPA does not apply (eg, against an individual acting in a personal or domestic capacity).

4.2 Data Protection Remedies

The PDPA provides for a range of administrative, civil, and criminal remedies, giving the PDPC broad enforcement powers.

Pursuant to sections 48I and 48J of the PDPA, the PDPC may issue directions requiring an organisation to stop collecting, using or disclosing personal data, to destroy personal data, to implement policies and practices, or to pay a financial penalty. The maximum financial penalty is 10% of the organisation's annual turnover in Singapore for organisations with annual local turnover exceeding SGD10 million. For smaller organisations, the cap remains SGD1 million. The applicable penalty/fine depends on the severity and scale of the breach, the organisation's level of culpability and its remedial steps.

Civil damages are available under section 48O of the PDPA, which provides individuals with a private right of action for loss or damage suffered as a result of a contravention of the PDPA by an organisation or data intermediary. A prior finding by the PDPC is not a prerequisite to bringing a private civil action, meaning individuals may proceed directly to court. Injunctive relief is also available through the civil courts in appro-

prate cases, particularly where ongoing or threatened breaches are in issue.

Criminal liability is also applicable for certain egregious conduct. It is an offence under the PDPA to knowingly or recklessly use personal data obtained without the owner's consent (section 48E of the PDPA), make access requests for personal data without authority (section 51 of the PDPA) or disclose personal data obtained without consent (section 48D of the PDPA). Penalties include fines of up to SGD5 thousand and/or imprisonment of up to two years for individuals, with enhanced penalties for repeat offenders and corporate liability for offences committed by employees.

If it can be established that the data constitutes confidential information and a breach of confidence is made out, remedies that may be granted include injunctions, delivery up, destruction and/or damages.

The PS(G)A imposes criminal penalties on public officers who, without authorisation:

- knowingly or recklessly disclose data;
- misuse data that results in personal gain for the public officer or another person, or harm or loss to another person; or
- knowingly or recklessly re-identify anonymised information.

It also imposes penalties on contractors and/or employees of contractors who misuse data. In these circumstances, the offender could be liable to a fine up to SGD5 thousand and/or to imprisonment of up to two years.

The quantum of financial penalties or damages is largely dependent on the facts.

For instance, financial penalties imposed by the PDPC have a wide range. For example, Marina Bay Sands was fined SGD315 thousand in October 2025 for a breach affecting over 665,000 individuals arising from inadequate controls during a system migration. The fine is the second-highest amount meted out by the PDPC, after the SGD750 thousand fine on Integrated Health Information Systems (IHiS) for lapses in securing patient data that resulted in the nation's worst data

breach in 2018. Lower penalties are more likely for smaller-scale breaches or companies.

For civil damages under section 48O of the PDPA, Singapore's data protection litigation remains nascent, and damages awards in reported civil cases have been modest, with no established quantum.

4.3 Data Protection Deadlines and Exemptions

The PDPA does not prescribe a specific limitation period for complaints to the PDPC. While there is no express statutory deadline, complainants are generally advised to raise concerns promptly and to attempt resolution directly with the organisation before escalating to the PDPC. The PDPC retains discretion on whether to investigate, and timeliness of the complaint is a relevant consideration.

For private civil actions under section 48O of the PDPA or a civil claim for a breach of confidence, the general limitation framework under the Limitation Act 1959 applies. Generally, depending on the exact claims made in any action, the typical limitation period is six years from the date on which the cause of action accrued – generally the date the contravention occurred, or, if applicable, the date the individual discovered, or could reasonably have discovered, the breach. Other timelines may apply for other specific claims, for example where claims involve allegations of fraud, mistake or personal injury.

A data intermediary, being an organisation that processes personal data on behalf of and for the purposes of another organisation pursuant to a written contract, has more limited direct obligations under the PDPA, pursuant to section 4 (2) of the PDPA. A data intermediary is directly bound only by the obligations to protect personal data, retain personal data, and notify the principal organisation of data breaches under section 24, 25, 26C and 26E of the PDPA. Liability for the remaining obligations rests with the principal organisation that engaged it. This is a meaningful distinction in outsourcing and cloud service arrangements, though it does not absolve data intermediaries of contractual liability to their principals.

4.4 Data Protection Proceedings Forum Choice

The primary forum for data protection enforcement in Singapore is the PDPC, which investigates complaints and may also conduct investigations on its own initiative. PDPC decisions may be reconsidered by the Commission itself, and thereafter appealed to the Data Protection Appeal Committee (“DPAC”) and further to the High Court on questions of law or on the amount of financial penalties (section 48R of PDPA).

Private civil actions under section 48O of the PDPA are brought in Singapore’s civil courts. There is no requirement to have first obtained a PDPC finding before commencing a civil action, though a prior PDPC decision finding a contravention may be persuasive in civil proceedings. A civil action may also be brought for a claim in breach of confidence.

Criminal prosecutions under the PDPA’s egregious misuse provisions are brought by the Public Prosecutor in the criminal courts. Unlike the administrative or civil routes, criminal proceedings require proof beyond reasonable doubt of knowing or reckless conduct and are reserved for the most serious contraventions.

Anonymity/Privacy of Data Protection Proceedings

Administrative proceedings by the PDPC are conducted confidentially, though PDPC decisions and financial penalties are typically published on the PDPC’s website and form part of the public enforcement record. Civil proceedings are generally public, with judgements published in the usual way. Criminal proceedings are generally open to the public, unless the court orders otherwise.

Singapore courts do not as a matter of course grant anonymisation orders or hear data protection claims in private. An applicant seeking such relief would need to satisfy the court that there are compelling grounds to do so.

Grounds Required to Bring Proceedings

The PDPA applies to organisations that collect, use or disclose personal data in Singapore.

Further, jurisdiction is generally established by the personal service of originating process on the defendant.

In the alternative, it might be established by substituted service or service outside of Singapore (subject to the court’s approval).

4.5 Data Protection Costs

Singapore civil litigation follows the general common law principle that costs follow the event, ie, the successful party is ordinarily entitled to recover a proportion of legal costs from the losing party. This principle applies to civil actions under section 48O of the PDPA, in the same way as any other civil claim. Cost orders are at the court’s discretion and are assessed on either a standard basis (being reasonable costs reasonably incurred) or an indemnity basis (being all costs save those unreasonably incurred).

In practice, cost recovery in Singapore civil litigation is partial. Assessed costs on the standard basis typically recover only a fraction of actual legal costs, with the remainder paid by the party who incurred them.

5. Regulatory and Media Environment

5.1 Key News Providers

According to *Reuters’* Institute Digital News Report 2025, trust in the news in Singapore stood at 45%, with *The Straits Times* (75%), *Channel NewsAsia* (74%), and *Mediacorp’s Channel 5* (73%) ranking among the most trusted news sources. Five of the most influential news providers, and a brief assessment of their approach to privacy, accuracy, and journalistic ethics, are as follows:

- *Channel NewsAsia* (“CNA”), owned by *Mediacorp*, is Singapore’s most used online news source, with a weekly reach of 47%. CNA generally maintains high standards of factual accuracy and editorial professionalism, especially on international and economic matters.
- *The Straits Times*, owned by *Singapore Press Holdings* (“SPH”), is Singapore’s flagship English-language broadsheet. It is the “newspaper of record” and maintains generally accurate and well-sourced reporting.
- *MotherShip* is a digital-native outlet with strong online reach, particularly among younger Singa-

poreans. Naturally, alternative and independent outlets continue to lag behind in public trust.

- *Lianhe Zaobao*, owned by *SPH*, is Singapore's flagship Chinese-language daily and the primary news source for the Mandarin-reading community. It maintains generally reliable factual accuracy.
- *The Business Times*, owned by *SPH*, is the primary source of financial and corporate news. It maintains high standards of factual accuracy on financial matters and is subject to the same structural editorial constraints as *The Straits Times*, given their common ownership with *SPH*.

In general, Singapore's newscasters have not been associated with significant privacy or ethical controversies. There is no press-specific privacy code equivalent to the UK's Editors' Code of Practice in Singapore.

5.2 Regulatory Framework

The primary regulator for broadcasting and content in Singapore is the Infocomm Media Development Authority ("IMDA"), established under the IMDA Act 2016 as a converged regulator for the info-communications and media sectors.

The key legislative instruments are:

- the Newspaper and Printing Presses Act 1974, which governs newspaper licensing and ownership;
- the Broadcasting Act 1994, which governs broadcast licensees and underpins IMDA's content codes;
- the Protection from Online Falsehoods and Manipulation Act 2019 ("POFMA"), which empowers ministers to issue corrections and stop communication directions against online falsehoods; and
- the Foreign Interference (Countermeasures) Act 2021, which addresses hostile foreign information campaigns.

Broadcasters or online news sites with significant local reach are required to obtain individual licences from IMDA. Licensees are required to comply with relevant codes of practice published by IMDA.

Singapore's regulators are effective in protecting public institutions. The framework does not formally protect media outlets from legal action, and there is no constitutional press freedom guarantee.

5.3 Complaints Process

The complaints process in Singapore operates across several distinct regulatory channels depending on the nature of the content and the platform involved.

For broadcast and online content, complaints may be lodged with IMDA, which has powers to investigate licensees for breaches of the applicable content codes. IMDA may direct a licensee to remove or prohibit the broadcast of content that is contrary to a code of practice, against the public interest or public order or offensive to good taste or decency. Sanctions include formal warnings, financial penalties and in serious cases suspension or revocation of a licence.

For online falsehoods, any member of the public may apply to the POFMA Office for a direction or declaration under POFMA where they believe a false statement of fact has been communicated in Singapore. POFMA's primary tool to correct falsehoods is correction directions under section 11 of the POFMA, which requires recipients to insert a notice against the original post with a link to the government's clarification, without the original post being removed. In more serious cases, stop communication or disabling directions may be issued (see sections 12 and 22 of the POFMA). The POFMA also allows for various criminal sanctions. For instance, offenders who communicate a false statement of fact that is likely to have serious consequences (eg, prejudice the security of Singapore) may be liable to fines of up to SGD100 thousand and/or imprisonment of up to ten years for individuals, and fines of up to SGD1 million for non-individuals under section 7 of the POFMA.

For data protection-related complaints arising from media activity, complaints may be lodged with the PDPC in the usual manner, subject to the PDPA's scope and exemptions.

5.4 User-Generated Content

Singapore does not have a statutory safe harbour equivalent to that in the US or EU that broadly shields

platforms from liability for user-generated content. The position is therefore governed by a combination of general law principles (eg, publication and/or republication of defamatory or false statements, joint tortfeasorship) and sector-specific regulatory obligations – websites may potentially be exposed to liability through such means.

For example, a platform or website operator may be exposed to liability for user-generated content on principles of secondary or accessory liability, where it has actual or constructive knowledge of the infringing or unlawful content and fails to act upon it.

From a regulatory perspective, IMDA-licensed internet service providers (“ISPs”) and content service providers are subject to the Internet Code of Practice, which imposes obligations to remove content that is contrary to the public interest, public order or national harmony. Designated social media services subject to the Code of Practice for Online Safety are required to implement systemic content moderation mechanisms, user reporting tools and proactive detection of specified harmful content categories, including child sexual abuse material, terrorism content and cyberbullying. Non-compliance is subject to financial penalties of up to SGD1 million.

Under Part 4 of the POFMA, internet intermediaries, including platforms hosting user-generated content, may be directed to apply correction notices to specific pieces of content, or to disable access to declared online locations. The intermediary is not required to remove the original content, but must display the correction notice prominently, and may be required to disable access to end-users in Singapore. Prescribed internet intermediaries are also subject to codes of practice issued by the POFMA Office, requiring them to undertake “reasonable due diligence” methods to, amongst other efforts, have systems in place to deprioritise online falsehoods.

5.5 SLAPPs

Singapore does not have dedicated anti-SLAPP legislation, and there is no statutory mechanism specifically designed to enable the early dismissal of claims identified as abusive or intended to chill public interest reporting.

The tools available in such abusive or vexatious litigation are based again on general principles or specific regulatory provisions for the relevant platform. For example: applications can be made under the Singapore Rules of Court 2021 to strike out proceedings, on the grounds that the claim discloses no reasonable cause of action, is an abuse of process or is otherwise frivolous or vexatious. The bar for summary decisions (eg, striking out applications) tends to be high.

5.6 Preventing Foreign Judgments

Singapore does not have specific legislation equivalent to the US SPEECH Act 2010 that is designed to prevent the enforcement of foreign judgements in media or defamation cases. The enforcement of foreign judgements in Singapore is governed primarily by the Reciprocal Enforcement of Foreign Judgments Act 1959 (“REFJA”), and in respect of exclusive choice of court agreements, the Choice of Court Agreements Act 2016 (“CCAA”), which gives effect to the Hague Convention on Choice of Court Agreements. For countries not within these regimes, enforcement is pursued at common law.

Trends and Developments

Contributed by:

Tony Yeo, Kelvin Tan, Gary Low and Meryl Koh
Drew & Napier LLC

Drew & Napier LLC has been providing exceptional legal service and representation to discerning clients since 1889. It is one of the largest law firms in Singapore. Drew & Napier's defamation practice is part of the firm's dispute resolution practice, which is widely recognised as a frontrunner in the industry. The practice is sought out by high-profile individuals and companies, including international corporations,

banks and other financial institutions, for advice and assistance on defamation-related issues. The firm's lawyers are involved in many major and landmark defamation disputes in Singapore and are constantly breaking new ground. They have experience advising and litigating on a broad range of defamation matters, including cross-border disputes and cases involving defamatory material spanning various forums.

Authors



Tony Yeo is the director of Drew & Napier's intellectual property department, and a director in our dispute resolution department. He also heads our healthcare and life sciences practice. Tony is a litigator with an active court practice who has acted as lead counsel in many complex matters, including numerous high-stakes litigation cases. In a defamation and malicious falsehood case, he successfully obtained a judgement for the highest amount ever recovered in the Singapore Court by a claimant, against an individual who made statements that he knew were false and which were found to be maliciously made.



Kelvin Tan has an active practice in commercial litigation and international arbitration. He leads Drew & Napier's contentious employment practice. He regularly assists corporate and executive clients protect their industry and professional reputations, both in litigation and in helping them form strategic approaches to safeguard against reputational damage via traditional and modern media and communications channels. Kelvin also helps clients with reputational concerns in various other areas, including shareholder and fiduciary duty disputes, fraud, false advertising, passing off and impersonation.



Gary Low is involved in all areas of civil, commercial and criminal litigation and is co-head of Drew & Napier's criminal law practice group. He has acted in a wide variety of matters, including defamation claims and various banking, corporate and contractual disputes. He has also represented clients accused of diverse offences, including commercial crimes, corruption, money-laundering and securities offences, in addition to leading allegations into fraud, criminal breach of trust, breach of fiduciary duty, workplace harassment and other forms of misconduct.



Meryl Koh is a leading commercial litigator in Singapore, widely respected by peers for her expertise in complex civil and commercial disputes. She regularly advises high net worth individuals, public figures and household brands across the technology, video games, entertainment, sports and media industries. Her practice covers shareholder disputes, intellectual property matters, licensing conflicts, breaches of confidentiality, harassment claims and defamation actions. Meryl was part of the team that secured Singapore's highest damages award for malicious falsehood and defamation. She also successfully represented a YouTube personality with 26 million followers in a defamation suit against a media company and content creator.

Drew & Napier LLC

10 Collyer Quay
10th Floor Ocean Financial Centre
Singapore 049315

Tel: +65 6535 0733
Fax: +65 6535 4906
Email: mail@drewnapier.com
Web: www.drewnapier.com



Growth of Online and Social Media Defamation

The rise of social media has changed the landscape of public discourse. Ease of access and freedom of publication mean that any person can spread defamatory content online with ease. Defamation in established media such as newspapers or broadcast outlets is less common, though still relevant. A topical example is the recent high-profile defamation litigation between *Bloomberg* and two Cabinet Ministers.

Defamation now commonly involves publication on online platforms, including social networking sites such as Instagram, TikTok, Facebook and X (formerly known as Twitter), content websites and blogs, as well as private and messaging platforms such as WhatsApp and Telegram. Online platforms offer easy and widespread publication, enabling individuals to circulate statements instantaneously to a wide audience. As a result, the potential reach and impact of defamatory material is amplified compared to traditional forms of publication.

The court has consistently recognised that the speed, scale and persistence of online publications exacerbate reputational harm. Unlike print media, online statements can be accessed repeatedly, reshared across platforms and reproduced in different contexts long after the original publication. Singapore courts have also acknowledged the “percolation phenomenon”, where, as a consequence of modern technology and communication systems, a story has the capacity to “go viral” more widely and quickly than ever before, particularly where the subject matter concerns a person who is in the public eye (see *Lee Hsien Loong v Xu Yuan Chen* [2022] 3 SLR 924 (“*Lee Hsien Loong*”) at [87]).

One illustration of the dynamics and reach of social media defamation can be seen in *Lee Hsien Loong*. In that case, the Prime Minister of Singapore sued the editor of an online news blog, Xu Yuan Chen, for defamatory content published on the *The Online Citizen* website. The High Court noted that the impugned article had accrued 98,338 views in August 2019, and was viewed a total of 114,263 times between August and November 2019 (at [82]). The scale of dissemination was a material factor in assessing the seriousness of the defamation and the quantum of damages for defamation (at [85]).

The growth of online and social media defamation reflects a broader shift in the ecology of speech and reputation, and Singapore courts have recognised that online platforms materially intensify reputational harm through speed, reach and replicability. These considerations inform the courts’ assessment of general damages, considering that the breadth of dissemination bears directly on the gravity of the harm suffered.

The rise of online defamation has also led to legislative changes to add easier remedies. Amendments to the Protection from Harassment Act 2014 came into effect in 2020 to introduce a range of potential court orders targeted at false statements. These include the “Stop Publication Order”, “Correction Order” and “Disabling Order”, among others. The gist of these remedies are that upon proof that a published statement of fact is false, the court may order that the statement be removed or corrected if it is just and equitable in the circumstances.

Such remedies can be effective because they also enable action against the “internet intermediary” where the false statements of fact are published online on a service provided by that “internet intermediary”.

Cross-Border Reputation and Forum Issues

Online and social media communication is inherently borderless. In the digital environment, defamatory statements may be authored outside Singapore, published online, and yet cause substantial reputational harm within Singapore if accessed by readers locally. Social media platforms and messaging applications have blurred traditional territorial boundaries in the context of identifying where the tort of defamation happened, which raises complex questions of jurisdiction, the applicable law and natural forum.

A common issue in cross-border defamation is the identification of the place of the tort. Singapore adopts the double actionability rule in respect of torts like defamation, as reaffirmed by the Singapore court of Appeal in *Rickshaw Investments Ltd v Nicolai Baron von Uexkull* [2007] 1 SLR(R) 377. This means that a defamation claim is actionable in Singapore only if it is actionable both under the law of the forum (which would be Singapore if a claim is commenced in the Singapore courts) and under the law of the place where the tort was committed (the *lex loci delicti*).

In the context of online defamation, the place of the tort is the place where the defamatory material is accessed, read or downloaded by end users, rather than where it was uploaded or authored (see *Ng Koo Kay Benedict and another v Zim Integrated Shipping Services Ltd* [2010] 2 SLR 860 at [26]). Accordingly, where a statement is published on social media or other messaging services but is accessed by a person in Singapore and causes reputational harm here, the tort is arguably considered to have occurred in Singapore.

The Singapore court has demonstrated a willingness to exercise jurisdiction over such disputes where the factual matrix establishes a real and substantial connection to Singapore. For example, in *City Spark (Singapore) Pte Ltd v The Outdoor Recreation Group, LLC* [2025] SGHC 25, the defendant, who was based in the United States, sent an allegedly defamatory WhatsApp

message that was received and read by an individual in Singapore. The claimant alleged that this statement was defamatory. The US defendant attempted to stay the proceedings on the ground of forum non conveniens, contending that Singapore was not the appropriate forum. The High Court rejected the application and held that Singapore was the natural forum for the dispute. Applying the well-established *Spiliada* principles, the court found that Singapore had the most real and substantial connection to the action, because (among other things) the individual who was the recipient of the alleged defamatory WhatsApp message likely received the statement when he was in Singapore, and was a key third-party witness working and residing in Singapore, such that he could not be compelled to testify overseas in a US court (at [10]).

The High Court further held that difficulties in enforcing a Singapore judgement abroad did not displace Singapore as the appropriate forum. The burden lay on the defendant to demonstrate the existence of a clearly more appropriate alternative forum (at [5]), which they failed to do.

From a practical standpoint, this has significant implications for both claimants and defendants. Claimants with reputations in Singapore may seek redress in the Singapore courts, even in cases where the defamatory content originates overseas, assuming that the defamatory content was accessed in Singapore. Conversely, foreign defendants who publish statements accessible by a Singapore audience cannot assume that Singapore courts will decline jurisdiction merely because the publication was authored abroad.

AI and Defamation

An emerging development in the realm of defamation law relates to the increasing prevalence of AI-generated content. The ease of generating realistic false content using AI tools, such as deepfake photographs or videos, means that defamation involving AI-generated images or videos is likely to become significant and increasingly common.

Although the Singapore courts have yet to adjudicate defamation claims squarely involving AI-generated content, the issue has been considered in other jurisdictions. Existing principles of defamation, such as the

defamatory nature of the statement, reference to the plaintiff and publication, are likely to remain applicable. However, the application of these principles may require nuanced adaptation to accommodate the distinctive operational characteristics of AI systems.

Whether AI-generated content can be defamatory in nature

It is commonly acknowledged that AI-generated content carries an inherent risk of factual inaccuracy. Generative AI models, particularly large language models, operate on probabilistic mechanisms that prioritise linguistic coherence and plausibility over factual verification. As a result, such systems may produce output that appears to be correct but is actually inaccurate, misleading or wholly fabricated – a phenomenon commonly referred to as a “hallucination”.

Publicly accessible AI systems like ChatGPT are routinely accompanied by user warnings or disclaimers acknowledging that generated output may be incorrect, incomplete or unreliable. This suggests that users are, or ought to be, aware that AI-generated information cannot be accepted uncritically as fact.

The reality is somewhat less clear because anecdotally, the ordinary member of the public places some degree of trust in the content generated by an AI system. The extent of this trust varies from person to person, though it may be a stretch to say that the ordinary reasonable person has full awareness that AI-generated content may not be true. Instead, an ordinary reasonable person may believe that AI-generated content is likely to be accurate. By way of illustration, a global study by KPMG and the University of Melbourne found that 2/3rds of employees report “having relied on AI output at work without critically evaluating the information it provides”, and over half report having “made mistakes in their work from AI use” (at page 75). Further, there is a human tendency to over-rely on technology, including AI systems, which may result in a misplaced confidence in AI-generated content and a failure to independently verify its correctness.

From a legal perspective, this has implications when considering whether any AI-generated content is defamatory. The test to determine the defamatory meaning of a statement is by asking what an ordi-

nary reasonable person would understand the words to mean in the context of the offending publication. It is unclear whether an ordinary reasonable person, in reading any AI-generated content, would or would not believe that any AI-generated content was stating actual facts without attempting to verify it.

The Superior Court of Georgia in *Walters v Openai, L.L.C* (23-A-04860-2) adopted the view that a reasonable person who was aware from past experience that AI systems could generate fictional responses and received repeated disclaimers about the possibility of mistaken output, would not believe AI-generated content was stating “actual facts” without attempting to verify it. In our view, this assumption may go too far, given the anecdotal evidence that the current reasonable man has an imperfect understanding of how generative AI works, and it can equally be said that an ordinary reasonable person, when presented with AI-generated information, believes more often than not that the contents are statements of fact. This is likely to shift given that generative AI systems have only become widely available to the general public over the past few years.

It remains to be seen what approach the Singapore courts will adopt in respect of defamation involving AI-generated content.

Responsibility for AI-generated content

A further issue is the proper allocation of legal responsibility where defamatory content is generated by AI systems.

Given the way that generative AI models produce content, no single human actor exercises full control over what is generated. This is a paradigm shift from current content creation, where a human is responsible for words used or pictures drawn. Where a human provides an innocuous prompt that a generative AI model interprets by including false and defamatory statements of facts, how should liability be determined?

From one perspective, liability for defamation should still apply to the individual who published the AI-generated content online. This is clear where there is human involvement in the decision to take the AI-

generated content and publish it. The position is less clear with autonomous systems where an AI tool may be given the ability to publish its own content.

In this context, at least two categories of actors may be found legally responsible for AI-generated defamatory content.

- Deployers: they implement or integrate AI systems into products or services, whether through in-house development or third-party procurement.
- Users: they input prompts into generative AI systems and may influence, though not determine, the resulting output.

As AI models lack legal personhood, defamed parties cannot bring claims directly against them. In turn, this raises the question of whether the deployers and users who rely on and disseminate generative AI output ought to be regarded as liable for such content, in the same way that traditional news or media outlets are held liable for their publications.

With regard to deployers, jurisprudence from other common law jurisdictions indicates a willingness to impose responsibility on entities that present AI-generated information to the public as part of their services. In *Moffatt v Air Canada*^{2024 BCCRT 149} (“*Moffatt*”), the British Columbia Civil Resolution Tribunal held an airline liable for incorrect information provided by a chatbot on its website concerning bereavement fares. A customer of Air Canada had used the chatbot on Air Canada’s website to check his eligibility for the bereavement fare policy, and the chatbot gave him incorrect instructions on how to obtain the bereavement discount. The tribunal held that “[i]t should be obvious to Air Canada that it is responsible for all the information on its website. It makes no difference whether the information comes from a static page or a chatbot” (see *Moffatt* at [27]). While *Moffatt* was not a case involving defamation, the underlying logic suggests that deployers could arguably be found liable, where defamatory AI-generated content is disseminated through a product or service controlled and/or operated by the deployer.

From a different perspective, where a user intentionally prompts a generative AI system to produce defama-

tory content, the user is the party who has arguably created the content. The only step that matters is that they then take the content and publish it via a third-party. In that regard, the manner in which the defamatory content was produced is irrelevant.

A user/deployer that has published defamatory AI-generated content may, depending on the circumstances, avail themselves of various defences. This includes an offer of amends under section 7 of the Defamation Act 1957. This defence may be invoked if (among other things):

- the publisher did not intend to publish the defamatory content of and concerning that other person, and did not know of circumstances by virtue of which they might be understood to refer to him; or
- the words were not defamatory on the face of them, and the publisher did not know of circumstances by virtue of which they might be understood to be defamatory of that other person;
- the publisher exercised all reasonable care in relation to the publication; and
- an offer of amends is made.

A user/deployer that has published defamatory AI-generated content without any intent or awareness on their part and exercised all reasonable care in relation to the publication, such as by taking reasonable steps to cross-check AI-generated content, and have made an offer of amends, may be able to rely on this defence. It is less clear whether a user/deployer is entitled to rely on this defence if they failed to verify the accuracy of such AI-generated content.

As for defences of fair comment or qualified privilege, those are defeated by malice. In the context of using an AI-generated system, recklessness as to the truth may also constitute malice sufficient to defeat these defences.

Issues Arising from Deepfakes

With the advent of artificial intelligence, deepfakes have rapidly evolved into a serious digital threat. The fabrication of audio, video and images through deepfake technology can potentially constitute defamation where the content attributes certain false statements

or conduct to an individual, which subsequently causes reputational damage to said individual.

One example is an incident which took place in 2025, where a deepfake video was circulated of former President Halimah Yacob appearing to make negative comments about the Singapore government. Such deepfakes have the effect of potentially causing severe harm to the victim's reputation and may diminish the victim's moral or intellectual character in the eyes of others.

Singapore's legal framework is evolving to address the threat of deepfakes. Apart from defamation laws that protect victims whose reputations are affected by the circulation of deepfakes, the Protection from Harassment Act 2014 provides redress for victims of deepfakes who face distress.

In addition, the passing of the Online Safety (Relief and Accountability) Bill, which is expected to come into operation sometime in the middle of this year, will provide new measures to strengthen online safety and protect individuals from online harms by empowering victims to seek timely relief and obtain redress. For example, the Online Safety (Relief and Accountability) Act 2025 will introduce the statutory tort of "inauthentic material abuse", which would give victims of deepfakes recourse against communicators, administrators and platforms and allow victims to seek remedies from the court, such as compensatory damages and injunctions.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Luke.Wilson@Chambers.com