SMU
SINGAPORE MANAGEMENT UNIVERSITY

Yong Pung How School of Law

Report of the Online Harms Symposium: Exploring New Solutions and Legal Remedies for a Safer Online World

February 2025
Yong Pung How School of Law

CONTENTS

I. PREFACE 6

II. EXECUTIVE SUMMARY 9

III. THE ONLINE HARMS LANDSCAPE 15

A. THE PREVALENCE OF ONLINE HARMS 15

B. CONTRIBUTING FACTORS 20

1. The internet 20

2. Online anonymity 23

3. Tech companies 25

IV. CONSEQUENCES 33

A. VICTIMS 33

B. VULNERABLE GROUPS 40

C. THE LINK BETWEEN ONLINE AND OFFLINE HARMS 44

D. FREEDOM OF SPEECH, PUBLIC DISCOURSE AND REPRESENTATION 51

E. HARMFUL NORMS 58

V. A GLOBAL MOVEMENT TO ADDRESS ONLINE HARMS 61

VI. EXISTING MEASURES TO ADDRESS ONLINE HARMS IN SINGAPORE 67

1. Criminal offences 67

2. Regulatory measures 69

3. Civil remedies 70

VII. NEEDS AND POSSIBLE SOLUTIONS 74

A. SECURING THE EXPEDITIOUS REMOVAL OF ONLINE HARMS 74

B. IMPROVING THE ECOSYSTEM OF ACCOUNTABILITY 84

C. IDENTIFYING APPROPRIATE CATEGORIES OF ONLINE HARMS TO BE ADDRESSED 92

D. PROTECTING REPUTATIONS ONLINE 98

E. ADDRESSING ONLINE ANONYMITY 104

F. OTHER MEASURES 108

VIII. CONCLUSION 111

ONLINE HARMS SYMPOSIUM

Exploring New Solutions and Legal Remedies for a Safer Online World

Keynote Speech

Private Interests and Public Consequences: Understanding the Causes and Shaping the Future of Online Harms by Ms Frances Haugen

- Ms Haugen explored how private interests have trumped public interest in the design of internet platforms, and the impact this has had on online harms.
- Ms Haugen also shared her thoughts on solutions for reducing harm and promoting accountability on the internet.

Ms Frances Haugen
Advocate for Accountability & Transparency in Social Media

Panel Discussion 1

The Internet, Social Media and Online Harms: Global Solutions for a Vital Issue

- How have the characteristics of the internet and social media driven the proliferation of online harms, and what can be done about it?
- The panel discussed these matters and the steps that have been taken by private actors and countries around the world to deal with this vital issue.

Speakers

Ms Frances Haugen
Advocate for Accountability & Transparency in Social Media

Prof Lim Sun Sun
Vice President (Partnerships & Engagement), SMU

Dr Carol Soon
Principal Research Fellow, Institute of Policy Studies

Moderator

Ambassador Chan Heng Chee
Ambassador-at-Large, Singapore's Ministry of Foreign Affairs

Special Feature 1

Lived Experiences: How well do we understand the real-life impact of online harms?

- The proliferation of online harms has been a growing concern worldwide, and Singapore is no exception. As the use of the internet and social media platforms continue to dominate our daily lives, so too do the threats posed by cyberbullying, online harassment, hate speech, intimate image abuse and more.
- During this session, the clients of SheCares@SCWO, a counsellor from SheCares@SCWO and a youth advocate from Cyber Youth Singapore shed light on these issues through real-life sharing and case studies of victim stories – on the real-world impact of online harms on victims, both in Singapore and beyond.

Speakers

Lorraine Lim
Deputy CEO, SCWO & Centre Head of SheCares@SCWO

Xavier Low
Chief Executive, Cyber Youth Academy

Moderator

Simran Toor
CEO, SG Her Empowerment Ltd

Keynote Speech

Taking the Lead on Online Safety: Australia's eSafety Commissioner

- Australia's eSafety Commissioner is the world's first government agency dedicated to keeping people safer online.
- Ms Julie Inman Grant spoke on the origins and reasons for eSafety's formation in 2015, how it has grown to address emerging problems since then, and how it continues to successfully protect Australians from online harms.

Ms Julie Inman Grant
eSafety Commissioner, Australian Government

Panel Discussion 2

First Aid for Online Harms: Practical Steps to Take and How to Seek Help

- What should you do if you have experienced an online harm? Is there someone out there who can help?
- Ms Julie Inman Grant, Australia's eSafety Commissioner, and Ms Stefanie Yuen-Thio, Chairperson of SG Her Empowerment Ltd, shared practical steps that we can take and how organisations such as eSafety and SHECARES@SCWO can provide assistance.

Speakers

Ms Julie Inman Grant
eSafety Commissioner, Australian Government

Stefanie Yuen-Thio
Joint Managing Partner, TSMP Law Corporation, & Founding Chairperson, SG Her Empowerment Ltd

Moderator

Dean Lee Pey Woan
Dean, Yong Pung How School of Law, SMU

Panel Discussion 3

Reputational Harm in an Online World: Is Litigation the Best Medicine?

- The tort of defamation has been part of the common law for centuries. It has developed through the advent of the printing press and broadcast media. However, does it now sufficiently relieve the harm done by online defamation?
- This panel examined how online defamation differs from offline defamation, diagnosed what victims want to remedy the defamation, and prescribed possible solutions.

Speakers

Justice Philip Jeyaretnam
Judge, Supreme Court of Singapore

Prof David Ardia
Co-Director of the Center for Media Law and Policy & Assoc Prof of Law, University of North Carolina

Ramesh Selvaraj
Partner, Allen & Gledhill LLP

Moderator

Prof Gary Chan
Vice Provost (Faculty Matters), SMU

Panel Discussion 4

Understanding Online Harms: Archetypes, Prevalence and Impact

- "Online harms" has been the latest buzzword in tech and policy – and for good reason. These insidious and pervasive harms have proved capable of causing damage extending far beyond the online sphere, impacting the lives of victims and even affecting society at large.
- This panel unpacked "online harms" to better understand its archetypes and their prevalence in Singapore and around the world. The panel also explored the impact of such online harms, including how society and different segments within society are affected.

Speakers

Dr Chew Han Ei
Senior Research Fellow, IPS Social Lab

Simran Toor
CEO, SG Her Empowerment Ltd

Alexander Woon
Lecturer (Law Programmes), SUSS

Moderator

Assoc Prof Tan Seow Hon
Assoc Prof of Law, Yong Pung How School of Law, SMU

Special Feature 2

Ctrl + Alt + Del: Rebooting Online Behaviour

- With the rise of cancel culture and prevalence of hate speech, how can we still engage in dialogue meaningfully and respectfully online, even when we disagree?
- This Special Feature focused on the importance of constructive dialogue in multicultural Singapore.

Speakers

Liyana R Asmara
Head, Harmony Centre

Clarice Song
Founder, Bold at Work

William Wan
General Secretary of Singapore Kindness Movement

Moderator

Divian Nair
Founder/CEO of Storyteller Productions & Founder of We Are Majulah

Keynote Speech

Hate in the Modern Public Square

- Mr Damian Collins, MP described how the internet has become the public square of today, and what the impact of hateful content on the internet can have for society at large.

Damian Collins
Member of Parliament of the United Kingdom

Panel Discussion 5

Fostering Inclusive Online Spaces: Studying the Impact of Online Hate

- Individuals and groups attacked by hateful content can suffer severe harm, often extending offline.
- Societies may also feel the effects of polarization and alienation, with consequences for representation, diversity and the strength of the social fabric.
- This panel brought together a range of perspectives and explored issues pertaining to the nature of online hate and its pernicious effects on individuals, groups, and societies.

Speakers

Damian Collins
Member of Parliament of the United Kingdom

Dr Mathew Mathews
Head, Social Lab & Principal Research Fellow, Institute of Policy Studies, NUS

Asst Prof Karsten Müller
Asst Prof in Finance, NUS Business School

Moderator

Dr Carol Soon
Principal Research Fellow, Institute of Policy Studies

Panel Discussion 6

Redress for Online Harms: The Role of Legal Remedies

- How can legal remedies assist those who have been affected by online harms and what are their limitations?
- This panel discussed the availability, utility and limitations of legal remedies against online harms in Singapore and key foreign jurisdictions. It also discussed how the law can develop to address this evolving field.

Speakers

Goh Yihan
Judicial Commissioner, Supreme Court of Singapore

Prof Clare McGlynn
Prof of Law, Durham Law School

Prof Danielle Citron
Chapman Prof of Law, University of Virginia School of Law

Moderator

Assoc Prof Jason Grant Allen
Assoc Prof of Law, Yong Pung How School of Law, SMU

Panel Discussion 7

Disinhibition and Impunity: Anonymity on the Internet

- In the absence of overarching standards, rules regarding identification and anonymity are determined by the policies set by individual online platforms.
- Consequently, those who wish to remain anonymous and untraceable can easily do so.
- The panel discussed the psychology of online anonymity and the hurdles it poses for those who wish to seek redress.

Speakers

Adam Massey
Partner, C.A.Goldberg

Assoc Prof Eugene Tan
Assoc Prof of Law, Yong Pung How School of Law, SMU

Dr Tracy Loh
Senior Lecturer of Communication Management, SMU Lee Kong Chian School of Business

Ben Chua
CEO, Cyber Youth Singapore

Moderator

Prof Yip Man
Assoc Dean (Faculty Matters & Research), Yong Pung How School of Law, SMU

I. PREFACE

1 It is the core mission of the Singapore Management University Yong Pung How School of Law ("**YPHSL**") to address real world challenges that are of concern to society.

2 In recent years, it has become increasingly apparent that people are being subject to harm on the internet, ranging from long-standing forms of harm such as harassment and defamation, to more emergent forms such as cancel culture and deep fakes. Online harms are therefore a pressing social issue that requires collaborative partnership between policymakers, community stakeholders, industry actors and researchers across a variety of disciplines. Indeed, the SMU Centre for AI and Data Governance (now restructured as part of the Centre for Digital Law) has been studying the impact of technology with a view to formulating policy recommendations and governance frameworks to optimise its benefits whilst containing its harm.

3 We were therefore delighted to partner with the Ministry of Law to co-organise the Online Harms Symposium, which was held over three days from 25 to 27 September 2023. Convening the Symposium was Dean of YPHSL Professor Lee Pey Woan, with faculty members contributing as moderators for numerous panel discussions.

4 Speaking to the theme *Exploring New Solutions and Legal Remedies for a Safer Online World*, the Symposium brought together a distinguished slate of speakers and panellists from Singapore and around the world, including experts on online safety, lawyers and judges, academics, and representatives from community organisations. Together, the speakers and panellists identified key issues and challenges, and explored new solutions and legal remedies that are effective, swift and reasonably accessible.

5 The Symposium drew more than 160 attendees on each of its three days, comprising representatives from governmental agencies, lawyers, representatives from non-profit organisations, academics, and representatives from tech companies such as Amazon, Apple, ByteDance, Google, LinkedIn, Meta, Tiktok and

X (formerly Twitter). Many participated actively by posing questions to speakers and panellists and making their views known. An insightful and energetic discussion unfolded over the three-day proceedings, providing much food for thought.

6 In this report, YPHSL sets out some of the key themes that emerged during the Symposium and puts forward recommendations to better address the needs of those affected by online harms. The intent is to inform key actors such as policy makers and internet companies of extant needs, so that they may more effectively respond to the problem of online harms.

II. EXECUTIVE SUMMARY

7 Online harms are prevalent in Singapore. To give just one data point, a survey conducted by SG Her Empowerment ("**SHE**")[1] in 2023 found that 38% of respondents in Singapore have personally experienced online harms. For women and youths, the proportion is even higher.

8 Myriad factors contribute to this disconcerting statistic. A major determinant is the structure of the internet itself: in giving each of us the ability to freely express ourselves and reach countless others online, the internet has also allowed bad actors to easily target victims offline with a speed and lasting impact that is without comparison in history.

9 The way each of us uses and experiences the internet has not come about by mere happenstance. Unlike in the early days, where the internet was predominantly a decentralised network of websites, our experience of the internet is now influenced to a large degree by the tech companies whose online platforms comprise the current, more centralised structure of the internet. Thus, the decisions of large tech companies have an outsize influence on the prevalence of online harms. These include the policies by which they operate their platforms:

---

[1] SHE is an independent non-profit organisation with Institution of Public Character status, that strives to empower girls and women through community engagements and partnerships.

for example, allowing users to be anonymous and untraceable or amplifying content that drives strong user engagement. It also includes how they respond to instances of online harms: for example, whether they adopt appropriate policies and devote adequate resources to addressing online harms. On both these scores, the evidence indicates that there is much to be desired. Former Facebook employee turned whistleblower Ms Frances Haugen articulated the essence of the problem in observing that tech companies have prioritised profits over the safety of people.

10 Online harms have serious consequences for victims. Of the respondents to the SHE survey who reported having personally experienced online harms, 18% reported fearing for their own safety and that of others related to them; 15% reported having experienced mental health issues; and 10% reported having experienced physical health issues. Additionally, 31% experienced a range of negative emotions, such as anger, sadness, anxiety, embarrassment, shame, or helplessness.

11 Online harms also have less obvious but profound consequences for society. They undermine freedom of speech, in causing users to practice digital self-censorship or disengagement. When vulnerable groups, such as women and minorities, disproportionately experience online harms, their representation in society can be diminished and fault lines can emerge. Eventually, online harms

may become normalised, such that users become desensitised to their harmful effects and feel that they are to be tolerated as part and parcel of the online experience. The normalization of online harms may even lead to the normalization of similar offline behaviour.

12 What can be done to address these issues?

13 Over the course of the Symposium, the speakers highlighted deficiencies in the current framework for addressing online harms and suggested possible solutions to address them. Based on their feedback, we put forward a number of recommendations for policymakers and other stakeholders to consider.

14 First, it is necessary to **identify the specific types of online harms that require legal intervention.** "Online harms" as a label is both too broad and too vague for the purposes of legal reform. Among the many forms of online harms discussed during the Symposium were intimate image abuse and harms to reputation. These and other forms of harm will have to be carefully identified and defined. Indeed, even specific and more familiar terms such as "harassment" will need to be unpacked into discrete elements for the purpose of legislative definition.[2] Therefore, it is important to identify and clearly define the wrongful

[2] See sections 3 and 4 of the Protection from Harassment Act 2014 for an example of precise legislative language.

behaviours which are to be addressed. Further, as online harms are constantly evolving, it would be ideal for emergent forms of online harms and changing circumstances to be addressed in a timely way.

15 Second, there is a need to implement measures that appropriately address online harms. Most important is to secure **their expeditious removal from the internet**. Existing measures are clearly inadequate: for example, user reports of online harms to online platforms are frequently ignored or not dealt with expeditiously or adequately, and current avenues of legal recourse are inaccessible and costly. One possible way of expediting redress is creating **an agency empowered to receive complaints regarding online harms and issue legally enforceable directions to address those complaints**. That said, removal may not always be the most appropriate response to an online harm. Various speakers mooted the possibility of **allowing parties whose reputations have been harmed online the opportunity to respond to the offending statement swiftly and effectively**. Whatever measure is introduced, it must be accessible, swift, lasting and legally enforceable. In this regard, the Australian eSafety Commissioner provides a successful model for study and a useful template, with suitable modifications, for legal reform in Singapore.

16 Third, there is a need to **improve the accountability ecosystem**, which means holding those responsible for online harms accountable and enabling

victims of online harms to obtain redress. Accountability is central to the law of torts and familiar to all lawyers. Whilst the common law may develop incrementally over time to provide such an ecosystem, legislative reform through the introduction of **statutory torts** may be more appropriate in the circumstances as it enables a holistic review of the issues and thereby provides a more comprehensive and timely solution. This would entail identifying the online harms for which accountability and redress is required, providing clarity and certainty on potential causes of action and recoverable losses, and the parties to be held accountable.

17 Fourth, and importantly, it is necessary to **tackle the issue of online anonymity**. Online anonymity is repeatedly identified by speakers as a driver for online harms. Tackling this problem could entail providing more accessible alternatives to pre-action discovery as a means for victims to identify perpetrators of online harms, as well as requiring tech companies to collect more information from their users to ensure that they can be traced in the event that they perpetrate online harms.

18 Finally, we cannot merely rely on legal recourse and reform – be it regulatory, criminal or civil – to tackle online harms. Existing efforts to educate Singaporeans on digital literacy, the efforts that community organisations quietly undertake to support victims of online harms, and cross-sector conversations

about online safety are all important initiatives which must be continued and scaled. Further, members of society, as users of the internet, have a role to play in combatting online harms: we can start by being more gracious to one another and looking out for the occurrence of online harms.

III. THE ONLINE HARMS LANDSCAPE

19 Singapore has one of the highest internet penetration rates in the world. As of 2022, 99% of all resident households had access to the internet, and 100% of individuals aged 18 to 59 owned a smartphone.[3] Singaporeans of all ages and backgrounds use the internet to acquire knowledge, engage in public discourse, and express themselves.

20 The safety of the internet, or lack thereof, therefore directly impacts the well-being of Singaporeans. In this chapter, we examine the prevalence of online harms in Singapore and the factors which contribute to this phenomenon.

A. The Prevalence of Online Harms

21 In May and June 2023, SHE conducted a survey of 1,369[4] Singapore Citizens and Permanent Residents to better understand online harms. SHE Board Member, Dr Chew Han Ei[5] shared the results of this survey at a panel discussion on online harms.[6]

---

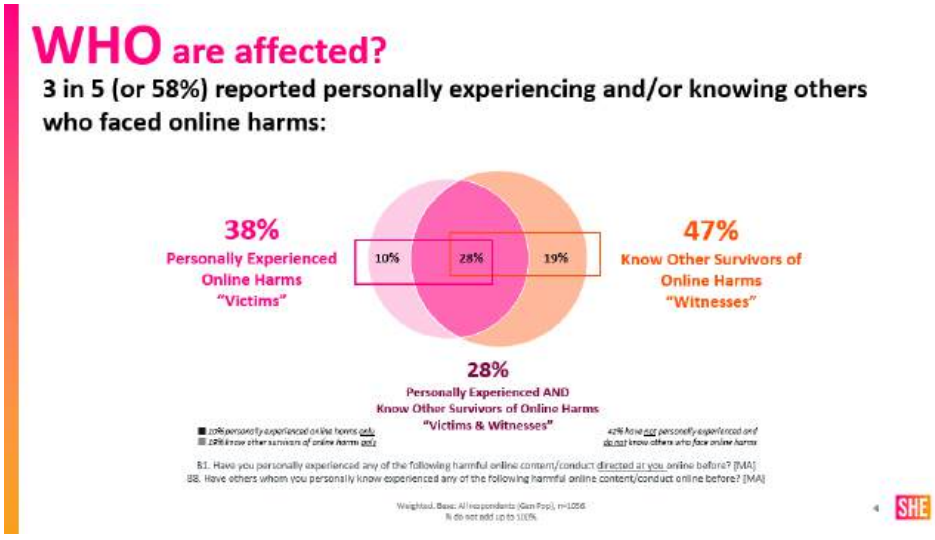
3 IMDA Annual Survey of Infocomm Usage by Individuals 2017-2022.

4 This comprised a main sample of 1,056 demographically representative respondents, and an additional 313 youths aged 15 to 34.

5 Senior Research Fellow at IPS Social Lab at the Institute of Policy Studies.

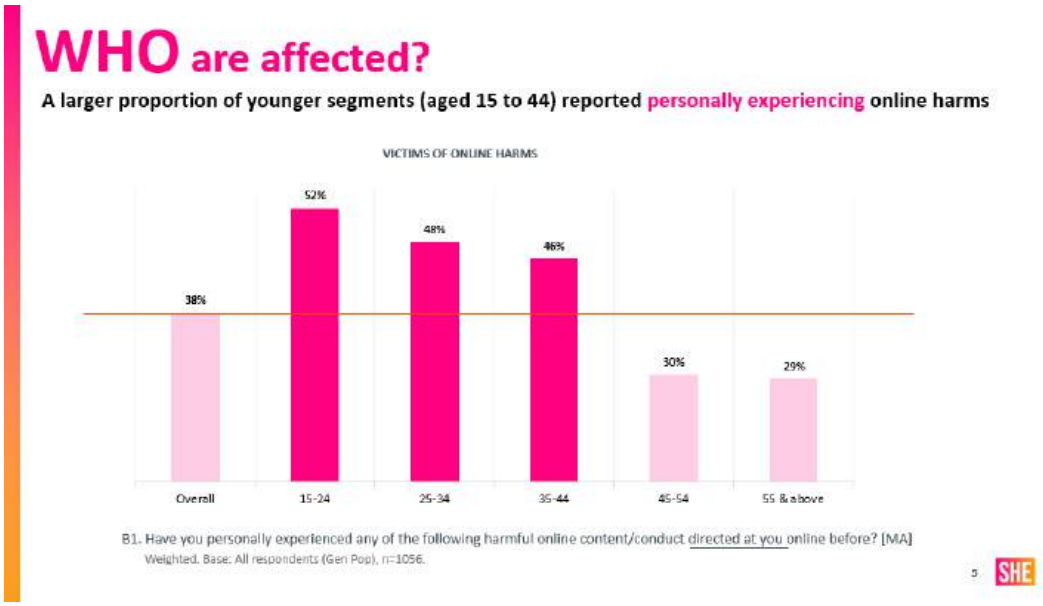
6 See also survey report available at: https://she.org.sg/news/she-study-reveals-majority-of-online-users-have-experienced-online-harms.

22 SHE's findings revealed the problem of online harms to be alarmingly widespread in Singapore, with 38% of respondents having personally experienced online harms and 47% known other survivors of online harms. 57% of respondents fell into one or both groups.



Credit: SG Her Empowerment.

23 This incidence of online harms varies across age groups. Younger respondents are more likely to personally experience online harms, with **more than one in two** respondents between 15- and 24-years old reporting having been victims of online harms.

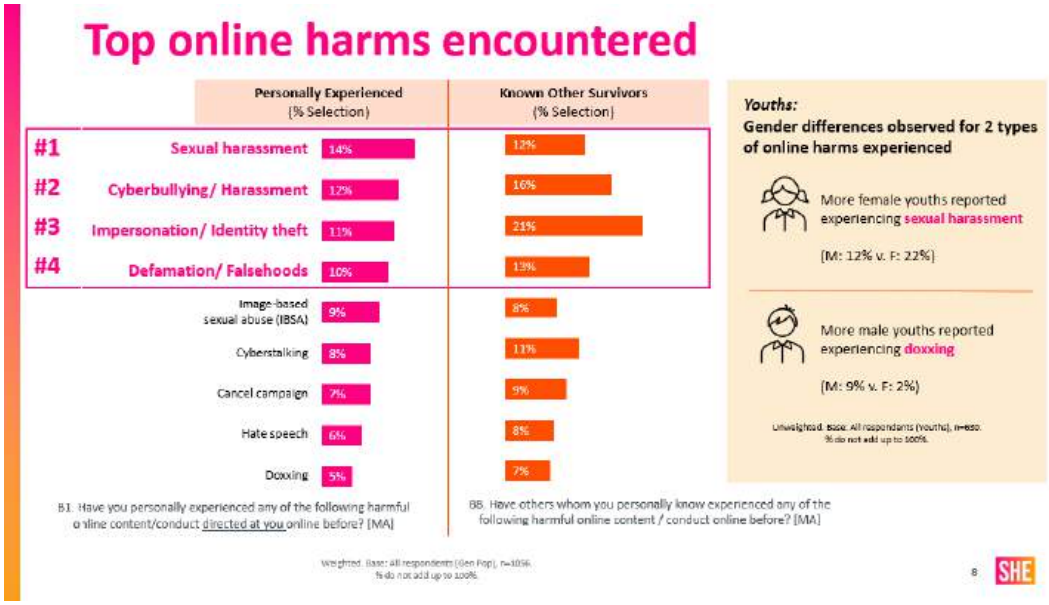


Credit: SG Her Empowerment.

24 The survey studied the prevalence of eight common types of online harms.[7] Of these, the most prevalent types are: (1) sexual harassment, (2) cyberbullying / harassment, (3) impersonation / identity theft and (4) defamation / falsehoods. Of

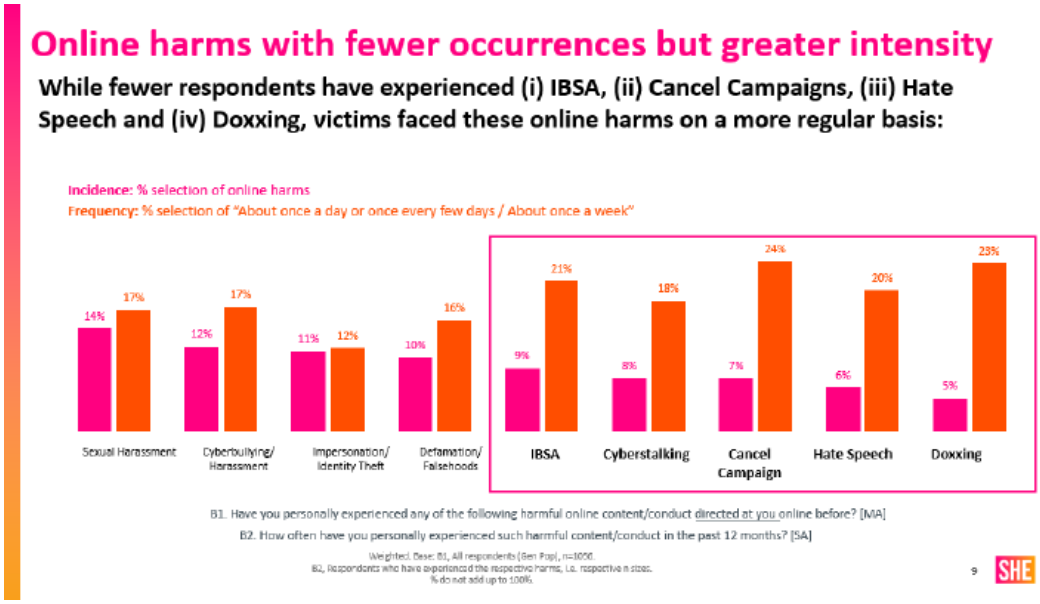
[7] Dr Chew Han Ei explained that the study did not cover online scams, which are highly prevalent, because these are already watched quite closely by the law enforcement agencies and lawmakers, and there are already official figures tracking the incidence of scams.

particular concern was the finding that 22% of female youths reported experiencing sexual harassment.



Credit: SG Her Empowerment.

25 While other forms of online harms may be less prevalent (*i.e.* there are fewer incidents), it does not mean that they are less concerning. Dr Chew shared that such online harms occur with greater intensity when they do arise, because victims experience them on a more regular basis.



Credit: SG Her Empowerment.

26 Moreover, less prevalent forms of online harms may also be extremely damaging when they do occur. This was implicitly recognised by the respondents of the SHE Survey, who regarded image-based sexual abuse as a top concern even though it was not reported to be prevalent.

27 The SHE survey is a timely addition to the slew of studies documenting the prevalence of online harms in Singapore and around the world. These include the 2022 poll[8] conducted by the Sunlight Alliance for Action in Singapore[9], the 2024

---

8 Sunlight Alliance for Action Report (August 2022).

9 Launched by the Ministry of Communications and Information in July 2021, the Sunlight AfA focused on closing the digital safety gap and establishing support mechanisms for victims of online harms. Co-chaired by SMS Sim Ann and SPS Rahayu Mahzam, it comprised 48 members from across the people, public and private sectors.

Microsoft Global Online Safety Survey[10], the 2020 study conducted by the Pew Research Centre[11] on the state of online harassment in the US, and the 2024 Online Safety Poll conducted by the Ministry of Digital Development and Information.[12] All these studies consistently demonstrate the existence of online harms at levels which raise concerns. We will return to the findings of the SHE survey later in this report.

B. Contributing Factors

28 Why are online harms so prevalent? Various speakers and panellists identified a number of contributing factors.

1. The internet

29 First, there is the nature of the internet itself, as enhanced and amplified by the vast and influential platforms which frame our interactions with the internet and each other.

---

10 Microsoft Global Online Safety Survey 2024.

11 Pew Research Center, "*The State of Online Harassment*" (13 January 2021).

12 MDDI, Online Safety Poll 2024.

30 To be sure, it was not always apparent that the internet would be a source of harm. Dr Carol Soon[13] noted that many utopic and hopeful aspirations were pinned to the internet when it first became mainstream, with visions of it levelling the playing field for individuals and marginalised communities, and of it giving everyone access to information.

31 While many of those positive aspirations have come to pass, the risks have also become increasingly clear. Dr Mathew Mathews[14] set out some of the main features of the internet which contribute to online harms, as augmented by the social media platforms through which most of us interact with the internet:

---

13 Principal Research Fellow and Head of the Society and Culture Development at the Institute of Policy Studies.

14 Principal Research Fellow and Head of the IPS Social Lab at the Institute of Policy Studies.

(a) **Anonymity**: online platforms often allow users to remain anonymous and thereby perpetuate a disinhibition effect. Indeed, online anonymity is such a pervasive issue that it merits closer scrutiny in the next section of this report.

(b) **Amplification**: algorithms can inadvertently prioritise sensational or polarising content.

(c) **Virality**: information spreads rapidly online.

(d) **Truncation**: online communication often lacks the non-verbal cues and context that are present in face-to-face interactions.

(e) **Insularity**: social media algorithms tend to show users content that aligns with their beliefs, creating an echo chamber effect.

(f) **Permanence**: online content exists forever because even when it is deleted from one platform, the content may have been screenshotted or a copy of it may be stored in a computer and uploaded again at a later date.

32 Many of these factors were highlighted by other speakers and panellists throughout the Symposium. For example, Dr Tracy Loh[15] spoke on how anonymity

---

[15] Senior Lecturer of Communication Management at SMU Lee Kong Chian School of Business.

and truncation embolden perpetrators of online harms, while Mr Ramesh Selvaraj[16] highlighted how the virality of online content has affected his clients. Professor David Ardia[17] explained the permanence of injurious information – the information remains in online data repositories and can be easily pulled out by a search engine.

2. Online anonymity

33 While each of the factors enumerated by Dr Mathews contributes to the prevalence of online harms, online anonymity is of particular salience and a panel discussion[18] was convened to discuss this specific issue. Indeed, it was a recurrent theme which ran through the entire Symposium, being repeatedly cited as a driver of online harms.

34 It must be noted at the outset that online anonymity does have merits. Dr Tracy Loh explained that anonymity allows people to speak their minds without fear of judgement or reprisal, including enabling them to seek help with issues they struggle with. It also allows people to be more honest and open, to express unpopular opinions or to speak on subjects that are regarded as socially taboo.

---

16 Partner and Deputy Head of International Arbitration, Allen & Gledhill LLP.

17 Reef C. Ivey II Excellence Fund Term Professor of Law, Co-Director of the Center for Media Law and Policy, and Associate Professor of Law, University of North Carolina at Chapel Hill.

18 *Disinhibition and Impunity: Anonymity and the Internet*.

These are undoubtedly positive effects of online anonymity which ought to be safeguarded.

35 However, Dr Loh also shared that the same disinhibition effect of online anonymity can contribute to online harms. Online users may feel less inhibited in behaving inconsiderately or badly because they do not witness the hurt that is caused to the victim. Nor are they at risk of physical retaliation. Crucially, many people believe that because they are anonymous, they will not get caught and therefore can do or say anything without regard to the harm that they may cause to others. This emboldens them to act with impunity and gives them a false sense of bravado. Echoing this view, Associate Professor Eugene Tan[19] opined that anonymity, impunity and disinhibition are closely related. In his view, more anonymity leads to greater disinhibition, which in turn leads to greater impunity.

36 Indeed, the sentiments of the expert panellists are consistent with the sentiments of lay persons who fall victim to online harms. Eve, a victim of online harassment, shared:

> *I think because she thinks I will never know who she is. This kind of like removed [her] identity – she's able to conceal herself behind a screen, behind a keyboard – so she was extra bold to speak her mind.*

---

[19] Associate Professor of Law at the YPHSL and former Nominated Member of Parliament.

37 While we may enjoy the anonymity we have on the internet, this feature also makes us vulnerable to online harassment by anonymous online users, including those who may impersonate us. Mr Adam Massey[20] shared about a client who had been subject to such a form of harassment. The anonymous perpetrator began by sending death threats to the police in his client's name, leading the police to show up at the latter's workplace. The anonymous harasser then used a plethora of personas on websites such as 4Chan, Reddit and Twitter to create a movement against her. As a result, the victim, her friends and family, and her employer were being contacted by people accusing her of racism and antisemitism.

3. Tech companies

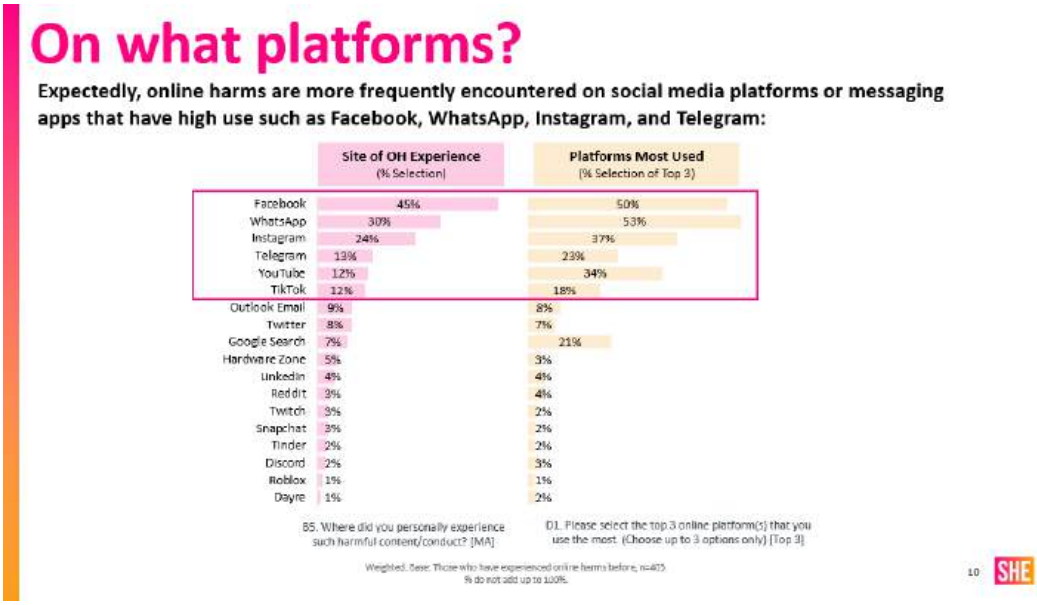
38 The use of the internet has changed markedly from its inception. In recent years, tech companies have had an outsize influence on how we experience the internet as we increasingly spend more time on social media.[21] Indeed, the SHE survey results show that online harms are generally most prevalent on the most-

---

[20] Partner, C.A. Goldberg PLLC, focusing on defamation defense, nonconsensual pornography litigation and sexual assault litigation.

[21] The Digital 2023 Global Overview Report published by Meltwater and We Are Social indicates that the average daily time spent on social media increased from 97 minutes in 2013 to 151 minutes in 2022.

used platforms, with Facebook, WhatsApp and Instagram taking the top three spots.



Credit: SG Her Empowerment.

39 Thus, the policies tech companies have regarding online harms have a significant impact on online safety. Unfortunately, the existing economic incentives are not aligned with the adoption of policies that enhance online safety.

40 Ms Frances Haugen, now an advocate for accountability and transparency in social media, explained in detail how tech companies have contributed to online harms.

41 In 2021, Ms Haugen released 20,000 pages of documents from Facebook's trust and safety organisation, allowing those outside social media platforms to

have a much better understanding of the issues involved. In her statement to the United States Senate Committee on Commerce, Science and Transportation at the time, Ms Haugen testified that Facebook's leadership knew ways to make Facebook and Instagram safer but would not implement the necessary changes because they have prioritised profits over the safety of people.[22]

42 While Ms Haugen's testimony related to Facebook, it is important to note that Facebook is not the only tech company that prioritised profits in decision-making. YouTube, for instance, has declined to modify its algorithms and reduce the filter bubble effect,[23] as the modified algorithm would result in lower watch times.[24] In the aftermath of the storming of the US Capitol on 6 January 2021, Facebook, Twitter (now X), Google, Snapchat and Twitch quickly took down harmful content inciting violence which had been hosted on these platforms for weeks. It has been observed that this was a "suddenly convenient decision made possible by a changed political landscape and new business imperatives".[25]

---

22 Statement of Frances Haugen to the United States Senate Committee on Commerce, Science and Transportation, 4 October 2021.

23 The term "filter bubble" was coined by Eli Pariser, and describes how algorithms can expose users to viewpoints they agree with and provide them with less exposure to conflicting viewpoints.

24 Foroohar, "*Don't Be Evil: The Case Against Big Tech*", Penguin Books (2019) at p 52.

25 Heidi Tworek, "*The Dangerous Inconsistencies of Digital Platform Policies*", Centre for International Governance Innovation, 13 January 2021.

43 Two years on from her Senate testimony, Ms Haugen remained firmly of the view that tech companies have solutions to address online harms but do not have the economic incentives to use them because these solutions would decrease the profitability of the platforms by small amounts.

> "*I believe the reason why this transparency is so important is because Facebook or TikTok, they have lots and lots of solutions. There are lots of solutions behind that curtain, but right now the economic incentives are such that they don't have motivation to use them.*"
>
> - Ms Frances Haugen

44 Drawing a comparison with the ecosystem of accountability that has brought the car industry into alignment with the common good by improving

safety, Ms Haugen observed that this did not happen for social media because of the information asymmetry between tech companies and everyone else. As a result, tech companies have been able to "spin any story they wanted to", and respond to instances of online harms by denying that systemic problems exist by describing any reported harm as anecdotal and not a representative experience on their platforms. Ms Haugen was not alone in this view. Professor Lim Sun Sun[26] expressed concern that the information asymmetry between industry on the one hand and policymakers and academia on the other is so great that we may have reached the point that we do not know what we do not know.

45 Contrary to their public averments, tech companies are aware of how their platforms contribute to online harms. According to Ms Haugen, by March 2021 Facebook knew through four of their own research studies that when users search for something moderate and follow the content that Facebook suggests, they will get pushed to extreme content over time. In spite of this knowledge, Nick Clegg, Facebook's then Vice-President of Global Affairs and Communications, claimed that users' experiences are shaped by their own choices and actions.[27]

---

[26] Professor of Communication and Technology and Vice President, Partnerships and Engagement at SMU.

[27] "You and the Algorithm: It Takes Two to Tango", Nick Clegg, 31 March 2021.

46 While content moderation has been touted by social media companies as a solution, it is not adequate and can even be counterproductive. Ms Haugen noted that content moderation brings about a modest 3-5% decrease in harmful content together with a large decrease of content intended to combat online harms. Further, it is considerably less effective for content that is not in English.

47 It should be noted that this was only one example of tech companies failing to act on user reports. This is a point which we will return to later in this report.

48 While Ms Haugen's speech was understandably focused on Facebook given her background as a former employee, her observations are of general relevance. For example, she expressed the opinion that Telegram, with its end-to-end encryption coupled with the ability to make mass broadcasts, was unquestionably the most irresponsible platform in the world.

49 The unfortunate reality is that all tech companies today are faced with the same tension between profit and safety, and some would choose to trade safety for profits.

50 Ms Haugen's observations were echoed by eSafety Commissioner Ms Julie Inman Grant[28]. Ms Inman Grant shared that when her organisation issued notices

---

[28] Ms Julie Inman Grant is Australia's eSafety Commissioner, the world's first government regulatory agency committed to keeping its citizens safer online.

requiring major tech platforms to disclose how they are fighting child sexual exploitation and abuse, it was discovered that some of the biggest, most wealthy and powerful companies were not deploying readily available safety technologies or enforcing their own terms of service. This was despite many of them having signed on to the Voluntary Principles to Counter Child Sexual Exploitation and Abuse[29], and claiming on a regular basis that they have zero tolerance for illegal content and harmful conduct.

51 In the context of hate speech, Mr Damian Collins, MP[30] observed that "*it is quite clear that the platforms are very well aware of the impact they have on the way news and information spreads and the way that can amplify hate, that there are adjustments they could easily make to these recommendation tools that would exclude some of the worst content, but they choose not to do it because it leads to a reduction in engagement*".

52 In a similar vein, Dr Carol Soon took note that the United Kingdom's newly passed Online Safety Act holds platforms to their terms of service. It seems

---

29 The Voluntary Principles to Counter Child Sexual Exploitation and Abuse were developed by Australia, Canada, New Zealand, UK and US, in consultation with six leading technology companies and a broad range of experts from industry, civil society and academia. It was launched on 5 March 2020.

30 Conservative Member of Parliament for Folkestone and Hythe from 2010 to 2024. Formerly the Parliamentary Under Secretary of State at the Department for Digital, Culture, Media and Sport, service as Minister for Tech and the Digital Economy in 2022; and Chair of the House of Commons Digital, Culture, Media and Sport Select Committee.

doubtful that such a legal obligation would have to be statutorily imposed if platforms were already complying with their own terms of service.

53 To be sure, the feedback on tech companies was not wholly negative. For example, SHE Chairperson Ms Stefanie Yuen Thio[31] observed that SHE has had a good experience working with the Singapore teams of tech companies.

54 However, the overall picture that emerged over the course of the Symposium proceedings is a grim one. Tech companies are in the position to do more to protect user safety but may choose not to because of economic disincentives, and the black sheep of the industry are less than fully candid about the trade-offs that have been made. Yet this is not a problem peculiar to tech companies as the same self-interested behaviour has been observed across a range of industries such as vehicles, tobacco, and fossil fuels. In our view, the way forward lies not so much in trying to find fault, but in recognising that the prevailing incentive structure is not aligned with promoting user safety. This is the root of the problem. The next step is to explore how private interests can be brought into alignment with the public interest of ensuring user safety.

---

[31] Ms Yuen Thio is also the Joint Managing Partner of TSMP Law Corporation and heads its corporate practice.

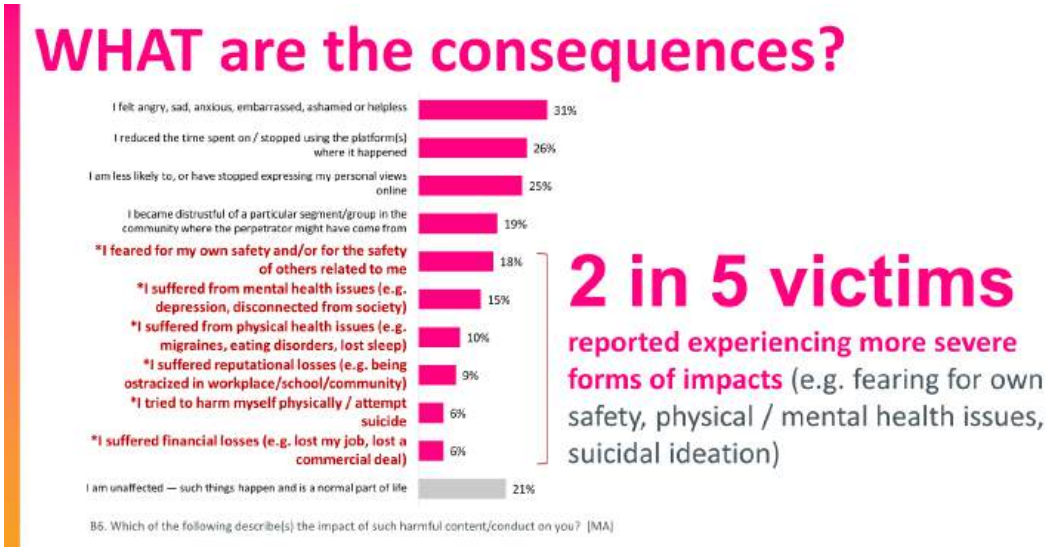
IV. CONSEQUENCES

55 We turn now to the consequences of online harms. This issue merits exploration because we need not be particularly concerned with the prevalence of online harms if the consequences are mild or insignificant. After all, it is not uncommon to hear online harms being described as “just online” or “not real”. Unfortunately, the evidence indicates that the consequences of online harms can be severe and can extend beyond the immediate victims to society at large.

A. Victims

56 We return to the SHE survey to understand the impact of online harms on their victims.

57 At the outset, it is worth noting that 21% of respondents who experienced online harms said that they were unaffected by it, viewing online harms as a normal part of life. However, this was not the case for the other 79% of respondents.



Credit: SG Her Empowerment

58 Of those affected, the most common impact (experienced by 31% of respondents) was the experience of negative emotions such as anger, sadness, anxiety, embarrassment, shame or helplessness. Some victims were so severely affected that they required support. Ms Simran Toor[32] shared about the strong demand for counselling services from victims who approach SHECARES@SCWO, a victim support centre set up by SHE in collaboration with the Singapore Council of Women's Organisations to help survivors of online harms.

59 Respondents also reported fearing for their own safety and that of others related to them (18%), as well as having experienced mental health issues (15%) and physical health issues (10%). Alarmingly, 6% of respondents reported having

---

[32] CEO of SG Her Empowerment.

tried to physically harm themselves or attempt suicide. This brings to mind the tragic examples of victims of online harms, such as Charlotte Dawson[33], who were driven by online abuse to take their own lives. Indeed, it is not difficult to find examples of such tragedies closer to home. In 2020, a 20-year-old Malaysian woman hanged herself after a video of her and a male colleague went viral and attracted derogatory remarks.[34]

60 We agree with Dr Chew Han Ei's observation that there are real people behind the statistics, and it should not take a tragedy to prompt action to address online harms. At the Symposium, several courageous victims shared their experiences with the attendees to remind us that online harms are real, persistent and have long lasting impact on the victims and their loved ones.

> **Eve**
>
> Eve was a victim of harassment, that included impersonation and cyberstalking, by an anonymous perpetrator. The harassment took place on multiple platforms, including professional networking platform, LinkedIn, which threatened to derail her career and personal life. The perpetrator was relentless in targeting Eve, bombarding her with abusive messages, creating fake profiles of Eve to insult her and using private information about Eve to harass her, amongst other acts of harassment. The prolonged harassment caused grave distress to Eve, who was perpetually anxious and

---

33 "*Charlotte Dawson's death puts cyberbullying back in spotlight*", ABC News, (23 Feb 2014).

34 "*20-year-old woman dies by suicide after allegedly being cyberbullied over her TikTok video*", Says.com (21 May 2020).

fearful for her safety, as she did not know who the perpetrator was and what else the perpetrator was capable of. She described herself as having become more withdrawn and wary of people after the incident, and she no longer feels safe sharing anything about her life online lest it be weaponised against her. Eve continues to suffer from anxiety and paranoia more than a year on, and has been attending counselling sessions to help cope with the trauma.

Andrew

Andrew was tricked into sending his intimate videos to a person he had met on an online dating application, whom he thought of as a potential romantic partner. The perpetrator later blackmailed Andrew with the videos, threatening to send them to his family and friends unless he paid up. It was only at that point that Andrew discovered the perpetrator was located overseas, and unlikely to have been the person she professed herself to be. He was very distressed and suffered from frequent acute anxiety attacks due to the fear of the videos being leaked, and even developed suicidal ideation. Andrew turned to counselling sessions to help cope with the incident, but is also resigned to the fact that the videos may be leaked any time in the future. As a result of the incident, Andrew no longer uses dating applications and is less active online.

61 The impact of cyberbullying can extend beyond the immediate victim. Ms Lorraine Lim[35] shared the stories of "Susan" and "Janet".

Susan

Susan had been harassed by her husband's mistress online for over two years. The harasser impersonated Susan and her child, posting abusive remarks and edited photos. Susan's parents and siblings also had their photos edited crudely and posted online. Eventually,

---

[35] Centre Head for SHECARES@SCWO and Deputy CEO of SCWO.

the victim's family ostracised Susan and blamed her for not being able to put a stop to the harassment. When Susan eventually approached SHECARES@SCWO for help, she was full of anxiety, hypervigilant and suicidal.

Janet

Janet had been the victim of image-based sexual abuse and felt shame and humiliation. Beyond Janet, her husband was also distressed, possibly more so than Janet, while her 9-year-old daughter was so angry with the perpetrator for ruining the lives of her parents that she wanted to physically harm him.

62 Based on the experience of victims who sought help from SHECARES@SCWO, Ms Lim observed that the consequences of online harms can be more serious than offline harms. She ventured the view that this may be due to a number of factors: harmful content cannot be completely deleted on the internet; victims are unable to walk away from cyberbullies unless they go offline completely; and the online harm may be seen by large numbers of people thereby causing a greater sense of shame and humiliation in the victim.

63 The impact is particularly pernicious where image-based sexual abuse is concerned and even worse when it involves child sexual abuse material. Ms Yuen Thio shared that when an explicit photograph of a person (whether genuine or a deepfake) is spread virally, "the first feeling is panic and the second feeling is more panic". Ms Inman Grant shared that 20% of child sexual abuse victims have been recognised by people on the street from the abuse material, and that image-based abuse follows the victims throughout the course of their lives and victims feel like they are constantly looking behind their shoulder.

"*The image can never be permanently deleted, so you have these girls doing reverse image searches on Google for the next 20 years of their lives, to see if the image is going to pop up again. They worry about 'when I grow up, can I be a CEO? What if this image comes back to haunt me? I can't be a politician, a judge.' They will discount themselves from opportunities because of what they fear is out there in the public domain about them.*"

- Ms Simran Toor

"*… intimate privacy violations and cyberstalking have profound cost to victims, in that it deprives them of jobs, they lose their jobs, they can't keep their jobs, it silences them and chases them offline. When I did my research, I interviewed 60 people from across the globe – US, Iceland, South Korea, Israel, India, and the UK, and the overwhelming response to intimate privacy violations was – the description was – it was like a life invasion, an incurable disease. That is, they can never stop looking for themselves online, because the next shoe to drop was, what's the next photo? What's the next post? Is*

> *someone going to impersonate me? And so, what we now have is absolute proof that intimate privacy violations, cyber stalking, what we can call digital forgeries, for example deepfake sex videos, causing incredible harm. It's undeniable.*"
>
> - Professor Danielle Keats Citron

64 It is crucial to consider seriously what this portends for the future. The SHE survey found that more than 1 in 2 of youths reported personally experiencing online harms while 2 in 3 know of someone who has been a victim of online harms. In the area of sexual abuse, Ms Inman Grant shared that the impact continues to persist throughout victims' lives, with a greater likelihood of them being sexually assaulted again, entering relationships that are abusive and/or committing offences themselves.

B. Vulnerable groups

65 Prevalent as online harms are, they do not affect us all equally. Some groups tend to be more vulnerable and more badly affected than others.

66 Ms Inman Grant noted that women are disproportionately affected by online harms because of the way abuse manifests against them: unlike abuse directed at men, abuse against women is sexualised and focused on their physical appearance, supposed virtue and fertility. A 2015 study by the UN Broadband Commission found that women globally are 27 times more likely to be cyber-

harassed than men.[36] This trend is reflected in Singapore. Writing in the Straits Times, Professor Lim Sun Sun and Dr Chew Han Ei have observed that women have encountered online content that is grossly sexist, misogynistic and laced with toxic masculinity.[37] Worryingly, the incidence is greatest for young women. The SHE Survey indicates that 22% of female youths have experienced sexual harassment, as compared to the rate of 14% across all respondents.[38]

67 Ms Inman Grant noted the spill-on effects into society if women self-censor or exit from public life or online discourse altogether, which will set gender equality backwards.

68 Besides women, children and youths are also vulnerable. The SHE survey found that the youngest age group surveyed (15–24-year-olds) also personally experienced the most online harms, with 52% reported having been victims. Consistent with this finding, in compiling the 2020 Child Online Safety Index, the DQ Institute found that 40% of children aged 8 to 12 and 52% of teenagers in Singapore were exposed to cyberbullying.[39]

---

36 Charlotte Alter, "*U.N. says cyber violence is equivalent to physical violence against women*", TIMES (24 September 2015).

37 Chew Han Ei and Lim Sun Sun, "*Online harm is an urgent issue for women*", The Straits Times (14 March 2022).

38 SHE Survey Report, page 12. However, it bears mention that more men reported personally experiencing online harms than women in the SHE Survey.

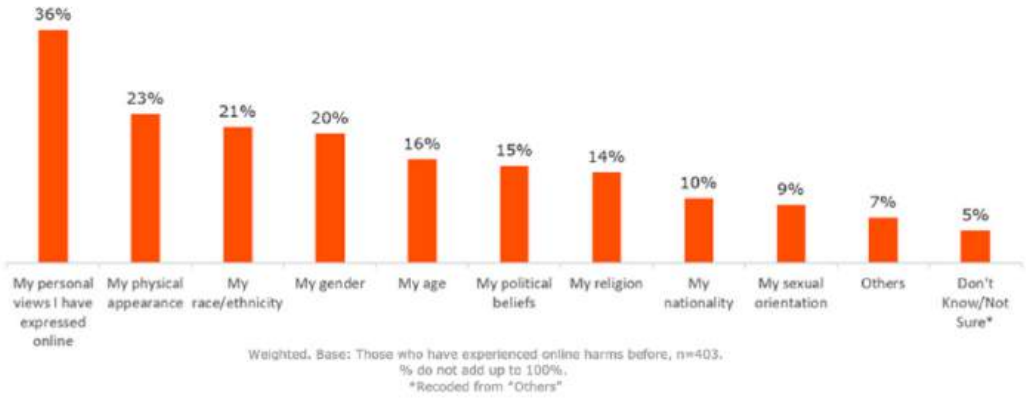
39 Yip Wai Yee, "*Singapore ranks 4th for best online safety for children: Survey*", The Straits Times (11 February 2020).

69 Further, Dr Carol Soon noted that survey findings, both local and overseas, show that marginalised communities such as racial minorities are particularly susceptible and vulnerable to online harms. In this regard, the SHE Survey found that 6% of respondents had personally experienced hate speech, while 8% know of others who have. Although this rate of occurrence may appear low in comparison to other types of online harm, Dr Carol Soon perceptively pointed out that this statistic must be considered in light of the laws and regulations Singapore has to address such conduct, such as the Sedition Act and the Maintenance of Religious Harmony Act.[40] Indeed, Ustazah Liyana Rosli Asmara, the head of Harmony Centre, an interfaith hub under the Islamic Religious Council of Singapore, noted that in other countries online trolls may actively promote online hate and suspicion among different religious groups. Therefore, the SHE Survey underscores the lasting potential for online harms to damage Singapore's social fabric.

70 Strikingly, many of the respondents to the SHE Survey reported that they believed they experienced online harms because of aspects of their identity. These identity traits included race / ethnicity (21%), gender (20%) and religion (14%).

---

[40] The Sedition Act was repealed on 2 November 2022, with the Ministry of Home Affairs explaining that its application was limited given the overlap with other laws such as the Maintenance of Religious Harmony Act, the Protection from Online Falsehoods and Manipulation Act, and specific provisions under the Penal Code. Plans have also been announced to introduce a Maintenance of Racial Harmony Act.



Credit: SG Her Empowerment.

71 Ms Inman Grant also noted that online abuse tends to be intersectional, with those from various minority backgrounds experiencing online abuse at double the rate of the general population.

72 It is important to recognise that the impact is not merely on the targeted group, but can extend to society at large. Mr Damian Collins, MP observed that hate speech is a very great danger to society today because it has the ability to turn groups in society against each other, to dehumanise people and to attack them because of their beliefs, *and* it may be carried out in an organised and systematic way through social media to create a pile-on effect.

C. The link between online and offline harms

73 While online harms take place on the internet, it would be incorrect to assume that the harm is only experienced there. In fact, there is often a link between online and offline harms.

74 The most commonplace spillover effect is victims fearing for their offline safety.

75 For example, Eve shared that she always felt anxious as her anonymous harasser had expressed knowledge of where she worked and lived, leading her to wonder whether she was being followed and if she would be physically harmed.

76 In more severe cases, online harms do travel offline. This was the case for Mr Massey's client whose anonymous harasser sent death threats to the police in her name, leading the police to show up at her workplace. The results can be far worse. In the US federal appeals case *Herrick v Grindr*, a former lover impersonated the victim on Grindr and claimed that he (the victim) wanted to engage in rape fantasies. Over a thousand people made unsolicited visits to the victim's home as a result. The victim filed more than fifty complaints with Grindr, which took no action.[41] In another case, a 28-year-old male from Wyoming posed

---

41 Carrie Goldberg, "*Herrick v. Grindr: Why Section 230 of the Communications Decency Act Must Be Fixed*", Lawfare (14 August 2019).

as his ex-girlfriend on Craigslist to claim she wanted to play out a "rape fantasy". This resulted in her being raped.[42]

77 Online harms do not just spill over into the offline world in respect of individual victims. The same can happen when groups (instead of individuals) are targeted. Mr Damian Collins, MP points out that history amply demonstrates that the normalisation of abusive speech and dehumanisation of other people lead to bad outcomes in the real world because what is delivered through speech becomes motivation for people to act violently.

78 Mr Collins' observation was given statistical backing by Assistant Professor Karsten Müller.[43] Professor Muller presented his research, jointly conducted with Assistant Professor Carlo Schwarz[44], which demonstrates that there is a causal link between online hate speech and offline hate crimes.

---

42 "*Jebidiah Stipe, Wyoming Marine, Solicited Ex-Girlfriend's Rape and Assault on Craigslist*", HuffPost (7 April 2010).

43 Assistant Professor of Finance, National University of Singapore Business School.

44 Department of Economics, Bocconi University.

79 Their research showed that there was a positive correlation between the number of anti-refugee posts on the Facebook page of the far-right German political party Alternative for Germany (AfD) and the probability of an attack on refugees, with the correlation stronger in towns with more intense right-wing social media usage. However, when a municipality experienced a major internet outage, the incidence of hate crimes markedly decreased notwithstanding the fact that the amount of anti-refugee posts circulating on the internet remained the same.

80 In Professor Müller's view, the only plausible explanation for the correlation of these events is a causal connection.

81 In the context of the US, Professor Müller shared that the incidence of anti-Muslim hate crimes occurred in areas where people use a lot of social media, and posited that the most plausible explanation for this phenomenon was that social media amplified offline violence.

82 Professor Müller opined that the data is evidence that what happens online does not stay there, and online conduct has real-life consequences. He stressed that societies should remain vigilant and not become complacent because the examples he had explored were largely unpredictable events that came as a shock to otherwise fairly rich and harmonious societies. The correlation between online hate speech and offline violence documented by Professor Müller is not unique to Germany or the US. Closer to home, there have been reports of

hate speech and hate crimes in countries such as India[45], Sri Lanka[46], Myanmar[47], and Indonesia[48].

83 Singapore is not exempt from these risks. Dr Mathew Mathews noted that there are potential fault lines in our social fabric based on race, religion, immigration, class and sexual orientation. In his view, online media increases the risk of fault lines emerging, due to the ubiquity of its use and consumption, alongside structural characteristics such as anonymity, amplification and virality. In Dr Mathew's view, when left unchecked, online hate can devolve into or engender more insidious outcomes including:

(a) **Radicalisation**: In extreme cases, online extremist content can radicalise individuals. Vulnerable individuals who come across such

---

45 "*Social Media's Role in the Violence in Jahangirpuri, India*, Manasa Narayanan", TechPolicy.Press, 13 December 2022; "*How these aggressive social media videos fuelled Haryana communal clashes*", Ankit Kumar, Arvind Ojha, Sreya Chatterjee, India Today, 2 August 2023.

46 "*In Sri Lanka, Facebook's dominance has cost lives*", John Harris, The Guardian, 6 May 2018; "*Sri Lanka accuses Facebook over hate speech after deadly riots*", Michael Safi, The Guardian, 14 March 2018.

47 "*Report of the independent international fact-finding mission on Myanmar*" (A/HRC/39/64) (12 September 2018); *A Genocide Incited on Facebook, with Posts from Myanmar's Military*, Paul Mozur, New York Times, 15 October 2018; "Myanmar: The Social Atrocity: Meta and the right to remedy for the Rohingya", Amnesty International, 29 September 2022; "*Facebook admit it was used to incite violence in Myanmar*", Alexandra Stevenson, New York Times, 6 November 2018.

48 "*Mob violence shows Indonesia must act against online hate speech*", Rido Parulian Panjaitan, The Conversation, 18 August 2016.

content may become more susceptible to extremist ideologies and even engage in violent acts.

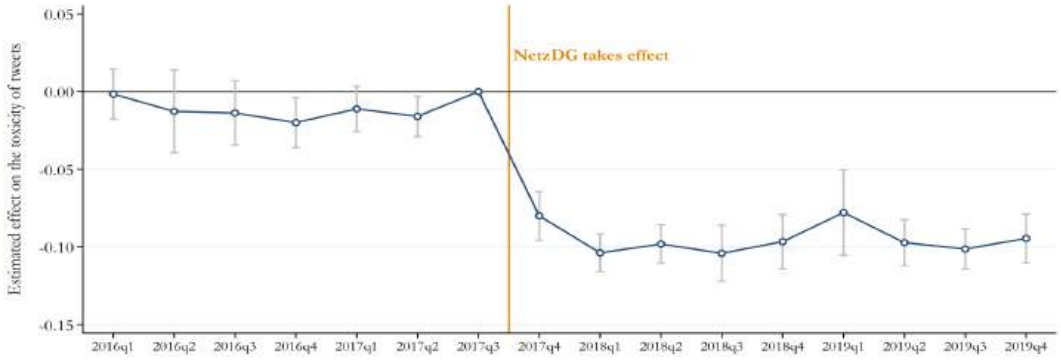
(b) **Polarisation**: Extremist speech can lead to the polarisation of different segments of society, deepening existing fault lines. It may create an "us vs. them" mentality, intensifying divisions along lines such as race, religion, nationality or sexuality.

(c) **Self-censorship**: Online hate may lead to self-censorship among individuals who fear retaliation or backlash. This can stifle open and honest discussions about important societal issues, and will impede social engagement endeavours.

(d) **Erosion of trust**: Prolonged exposure to extremist speech can erode public trust in institutions and authorities, including the government's ability to maintain social order and cohesion.

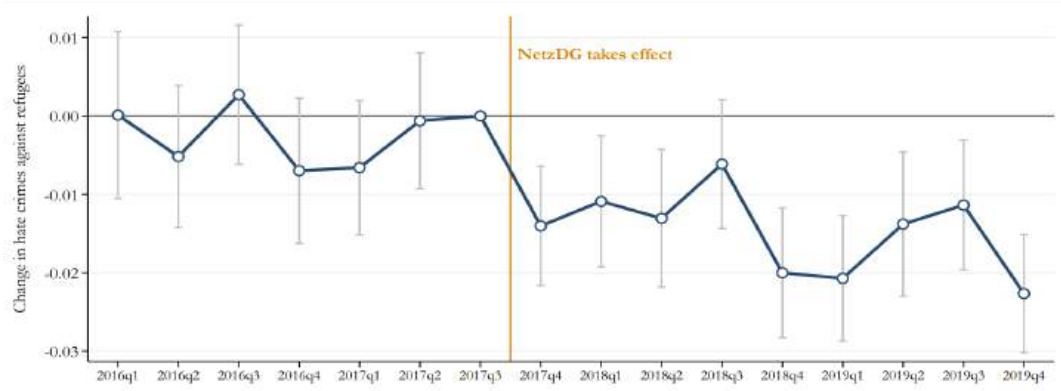
> "*We do enjoy general peace and harmony in Singapore, but that should not make us think that there are no fault lines. There are fault lines and they exist. If mismanaged and exacerbated, these have the potential to result in polarisation and conflict.*"
>
> - Dr Mathew Mathews

84 On a more positive note, Professor Müller demonstrated the positive impact of the German Network Enforcement Act (NetzDG), a law designed to address online hate speech. Professor Müller and his colleagues documented a reduction in the toxicity of online content after the law was passed.



Credit: Jiménez-Durán, Müller and Schwarz (2023).

85 At the same time, the incidence of offline hate crimes against refugees also decreased.



Credit: Jiménez-Durán, Müller and Schwarz (2023).

86 In our view, this change demonstrates the effectiveness and role of legislation in addressing online harms.

D. Freedom of speech, public discourse and representation

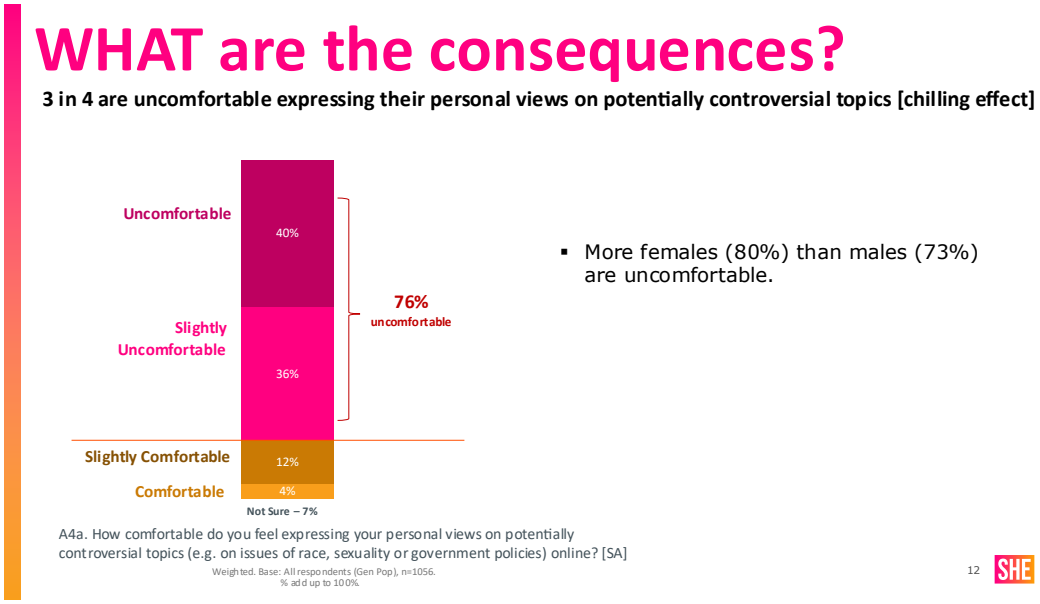
87 One of the common refrains raised when the idea of addressing online harms is discussed is that the proposed measures are attempts to regulate free speech.[49] Far less discussed is the effect online harms has on the freedom of speech. In Mr Collins' view, the other side of the story must be told: that is, some people are being denied free speech because they are intimidated to the point of avoiding online platforms altogether, or are being discouraged from speaking out because of the massive abuse they will be subject to.

88 Indeed, the SHE survey found that 3 in 4 respondents are not comfortable with expressing their personal views on potentially controversial topics online, with female respondents more affected than male respondents. Dr Chew explained that this is described as the "mean world syndrome" in the field of

---

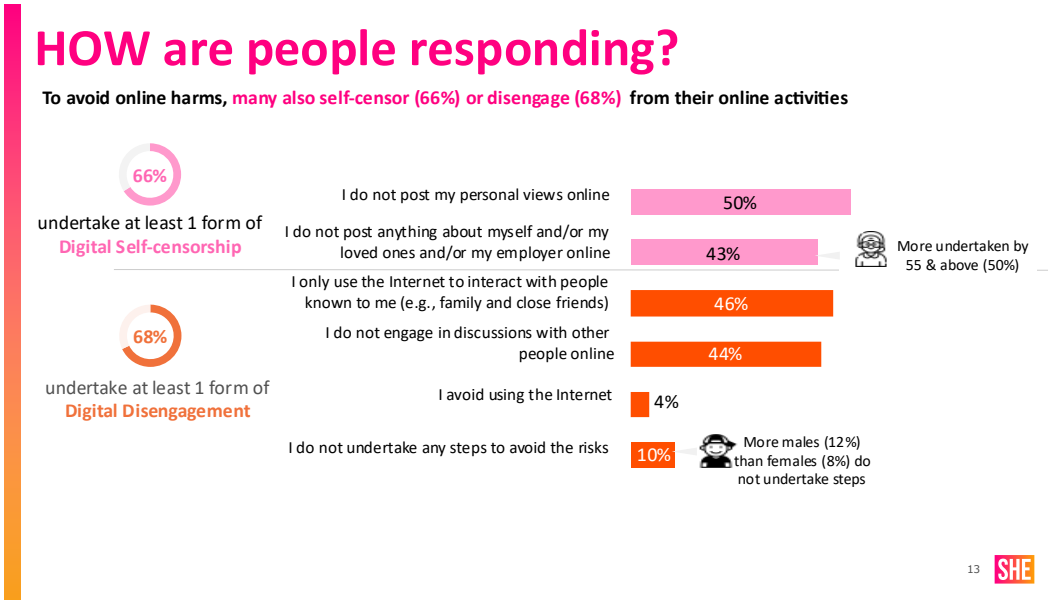
[49] See, for example, "*ORG warns of threat to privacy and free speech as Online Safety Bill is passed*", Open Rights Group, 19 September 2023; "*An unsafe bill: how the Online Safety Bill threatens free speech, innovation and privacy*", Matthew Lesh and Victoria Hewson, Institute of Economic Affairs, 27 June 2022; "*Germany: flawed social media law*", Human Rights Watch, 14 February 2018; "*Singapore's Online Safety Bill may be a double-edged sword, analysts say*", Dewey Sim and Kimberly Kim, South China Morning Post, 7 October 2022.

sociology, and that people refrain from online discourse because they are afraid of a lynch mob or being browbeaten for their views.



Credit: SG Her Empowerment.

89 To avoid online harms, 66% of respondents undertake at least one form of digital self-censorship, by refraining from posting their personal views online (50%) or posting anything about themselves, their loved ones and/or their employers (43%). 68% engage in at least one form of digital disengagement, by using the internet only to interact with people known to them (46%), refraining from engaging in discussions with other people online (44%) and avoiding the use of the internet (4%).



Credit: SG Her Empowerment.

90 This loss of freedom of speech and opportunity to fully engage online is *already* taking place because of online harms. And there is a danger that this problem may worsen. Ms Simran Toor observed that when young people go online and see other users being attacked or abused, it affects their trust and causes them to become fearful of the online space.

> "*… the social interest in countering harms is not just to protect individuals but to protect the social space for discourse.*"
>
> - Justice Philip Jeyaretnam

91 Beyond this, Dr Chew explained that if most Singaporeans are self-censoring or disengaging, we will be left with the very vocal minority who may have very extreme views. These extreme views are then amplified by social media algorithms and form the worldview of many moderate Singaporeans who do not expose themselves to different viewpoints.

> "*We must recognise that what people see on these devices is the lens through which they see the rest of the world and the people they are with and the communities they live in. And if that becomes an infected place, if the public square on this device is a bad place, then the public square in our towns and cities will become a bad*

> *place too. So, we need to make sure we act to keep people safe online, to deal with the worst offenders, to make the platforms liable for what happens, and … in doing that, we're working not just to keep our children safe, but our democracy and our societies safe and healthy as well.*"
>
> - Mr Damian Collins, MP

92 This is echoed by a 2018 paper published in the name of Facebook founder and CEO Mark Zuckerberg, which noted that:

> "*People will engage disproportionately with more sensationalist and provocative content… At scale it can undermine the quality of public discourse and lead to polarization.*"

93 This has knock-on impact for the sort of representation we see in society. The SHE Survey found that female respondents are more uncomfortable than men in expressing their views online (80% vs 73%). As Ms Inman Grant shared, if we want more parity in our legislative bodies and gender equality, there needs to be a greater understanding about how online misogynistic abuse targets women. Similarly, Dr Mathew Mathews commented that minorities that are targeted by abuse feel like they do not belong within society and tend to self-censor, being less willing to put forward their opinion because of the knowledge that they will be the target of hate. Another consequence observed by Ustazah Liyana is that groups which feel at risk of being targeted will create their own private spaces. Aside from diminishing the representation of such groups in society, this may also lead to online echo chambers.

94 Simply put, freedom of speech and public discourse are undermined even when online harms are *not* targeted at speech as such. However, there is evidence that online harms can deliberately be brought to bear against speech. Mr Alexander Joseph Woon[50] spoke on the phenomenon of Cancel Culture, which he described as weaponised peer pressure[51], which can be brought to bear against an individual in order to censor him for something he has said or done that is regarded by the canceller as unacceptable. Compounding the wrongfulness of the behaviour, cancellation can be implemented with other forms of online harms such as doxxing, harassment and image-based sexual abuse.

---

50 Lecturer, Singapore University of Social Sciences, School of Law.

51 See "*Cancel Culture and Freedom of Speech: Definitions, Effects and the Way Forward*", Alexander Joseph Woon, 2023.

95 Attacks which undermine freedom of expression are not merely brought to bear on individuals. Mr Collins gave the example of big pile-on campaigns attacking the media to undermine public confidence in the mainstream press when they seek to do their job by holding public figures to account for how they have behaved.

> *"[O]ur Parliament has empowered us to tackle online content that veers into the lane of online abuse with the intent to seriously harm the target, so the threshold is harm. I believe that this supports freedom of expression and healthy democracies by creating a more civil digital public square, and by offering deterrents to people who have previously abused without any repercussion. We've seen firsthand how online hate, harassment and abuse can undermine and hinder open democratic dialogue and debate, and promotes division and polarisation. It can have a chilling effect, leading to self-*

censorship and disengagement from public life and by discouraging political and civic ambitions."

- Ms Julie Inman Grant

96 It is worth asking why the freedom to commit online harms should be more valued than the freedom to use the internet without fear of becoming subject to them. It should further be asked why the freedom of speech for those who would commit online harms should be protected, when it is this very speech that deprives innocent internet users of their own freedom of speech.

E. Harmful norms

97 Multiple speakers have noted that online harms have become normalised and may in time lead to the normalization of *offline* harms.

98 Ms Simran Toor observed that while sexual harassment was perceived to be prevalent, it was not regarded as a top concern by most respondents of the SHE Survey. She posited that this could be because victims are starting to normalise this type of online harm and no longer identify it as harmful. In a similar vein, about 23% of respondents believe that in willingly posting something online one deserves any attack directed against oneself; and 16% of youths said that being sent unrequested sexually explicit images is acceptable.

99 Professor Lim Sun Sun observed that one of the findings made by the Sunlight Alliance for Action from speaking to people on the ground was that people do not necessarily report online harms either because they feel it is futile or because they do not recognise that something adverse has happened. The victim would process the wrongful conduct as something that happens to everyone and therefore consider it to be trivial in nature. Professor Lim opined that we should not allow society to fall into the trap of assuming that online harms are a necessary part and parcel of the online experience.

100 The normalisation of online harms is indirectly reflected in the fact that the victims seek help at SHECares@SCWO are the ones who are experiencing very serious harm. This indicates that those who experience less severe harm but who may nevertheless be in need of support are not coming forward.

101 Dr Chew noted that it has become quite normal in everyday life to hear of someone threatening to make those they are unhappy with "famous" and that the rules of interactions change if it becomes normal to use the threat of such a campaign to get what you want in society. It is disconcerting that some forms of online harms have become normalised to the extent that they are no longer regarded as being particularly harmful.

102 More pertinently, the potential for online harms to influence offline behaviour and social norms should not be overlooked. Mr Collins shared that there

appears to have been a return of racist chanting in football grounds together with online racist abuse of footballers. In a similar vein, Professor Müller stressed the importance of understanding how we should think about online content that is not necessarily toxic in any measurable way, but that may use codified language to spread fringe views which can have a major impact on social norms, and of what is normal or acceptable to say. In Professor Müller's view, such speech, which can be deeply sarcastic about particular groups and exclusionary in nature, has probably the most pernicious and corrosive impact on society, by making it completely normal to talk like that.

103 In our view, this underscores the need to build a common understanding that online harms are not acceptable.

V. A GLOBAL MOVEMENT TO ADDRESS ONLINE HARMS

104 Online harms present a different paradigm of wrongful conduct and damage to victims from offline harms. It calls for new and innovative policies and levers that can provide effective and timely solutions to victims.

105 Worldwide, different jurisdictions are responding with considerable urgency, reflecting a general consensus that online harms are a pernicious problem that need to be addressed. In a survey of regulatory measures enacted to address online harms, Dr Carol Soon noted the different approaches taken in laws passed in the European Union, the United Kingdom, the United States, Australia, and Asia (China, Japan, India, Indonesia, Malaysia and Thailand).

106 Some of the common legislative approaches include establishing an independent regulator to deal with online harms, introducing takedown and stop-communication directions; implementing measures to empower users through reporting mechanisms and tools to mitigate harms; imposing transparency requirements on tech companies in respect of how they handle online harms and users' experiences; and providing designated authorised persons who will be responsible for answering queries from the public and governments.

107 The European Union's Digital Services Act ("**DSA**") implements several approaches, by imposing obligations on platforms to make their services safer. These include:

(a) Implementing mechanisms to allow users to notify platforms about illegal content;

(b) Complying with orders from the authorities to act against illegal content;

(c) Publishing periodic reports on their content moderation efforts; and

(d) Appointing points of contact with the authorities and users.

108 The DSA also provides that users have the right to seek, in accordance with EU and national law, compensation from platforms in respect of any damage or

loss suffered due to an infringement by the platforms of their obligations under the DSA.

109 We elaborate below several insights shared by our speakers about the experiences in their respective jurisdictions.

110 Ms Julie Inman Grant, Australia's eSafety Commissioner, spoke about how her organisation contributes to making the online experiences of all Australians safer and more positive.

111 The eSafety Commissioner was set up in Australia in the wake of the tragic and high-profile suicide of a television personality named Charlotte Dawson. The regulator was initially set up as the Children's eSafety Commissioner, as it was widely agreed that children can be more vulnerable to online harms than adults. In the years since, the organisation was renamed the eSafety Commissioner, with its remit expanded in 2017 to cover all Australians.

112 The eSafety Commissioner's measures and powers include:

(a) Complaints schemes to address four categories of online harms: (i) cyberbullying of children, (ii) image-based abuse, (iii) adult cyber abuse, and (iv) illegal and restricted content. In administering these schemes, the eSafety Commissioner acts as a safety net when platforms fail to act on

reports of abuse, and bridges the power balance between the platforms and users who often do not have any recourse.

(b) Empowering educators and NGOs by equipping them with know-how to manage online harms incidents, and developing online safety standards.

(c) Preparing position papers which forecast looming tech trends and challenges, and help the Australian public understand how to protect themselves.

(d) Working with tech companies to create safer products through the Safety by Design philosophy.

(e) Holding tech companies accountable through the Basic Online Safety Expectations.

(f) Maintaining a register of industry codes and industry standards for illegal online material.

113 The eSafety Commissioner has been able to remove almost 90% of violative content, the vast majority of which were hosted overseas. This is commendable, not least because it can be challenging to compel tech companies in overseas jurisdictions to take action.

114 Mr Damian Collins, MP, shared five unique features of the UK's Online Safety Act 2023 ("**UK OSA**") which are intended to meet the challenge of regulating for online safety.

(a) The UK OSA establishes clear areas of criminal liability. For example, if platforms fail to comply with information requests from the regulator, this could attract fines of up to 10% of the platform's annual turnover.

(b) Platforms would be required to have systems in place to monitor and detect problematic content.

(c) Regulation would be based on codes of practice to be agreed upon between the regulator and each company.

(d) The UK OSA would require certain platforms to empower adult users to curate the content that is recommended to them, including avoiding content like hate speech and misogyny.

(e) In relation to messaging applications, regulators would be able to ask to see data that platforms already pick up in the background to help identify the worst offenders or worst criminal offences.

115 Professor Danielle Keats Citron,[52] a specialist in internet law, spoke about the discourse in the US on reforming section 230 of the Communications Decency Act of 1996, which currently immunises online platforms from liability for content posted by their users. This is significant because it demonstrates growing recognition, even in the US, that platforms should bear responsibility in protecting users from online harms and not be afforded absolute immunity from liability.

---

[52] Jefferson Scholars Foundation Schenck Distinguished Professor in Law and Caddell and Chapman Professor of Law at the University of Virginia School of Law.

VI. EXISTING MEASURES TO ADDRESS ONLINE HARMS IN SINGAPORE

116 In the last decade, various legislative measures have been introduced to tackle online harms. In particular, efforts have been made to modernise our criminal laws and regulatory measures, and step up digital literacy. Nevertheless, as we will explain below, a common thread that ran through the discussions at the Symposium is that more can be done to expand the range of remedies available to victims of online harm, as well as enhance their accessibility. We begin by outlining how existing laws deal with online harms.

1. Criminal offences

117 The Penal Code 1871 ("**PC**") and the Protection from Harassment Act 2014 ("**POHA**") identify specific online conduct that is punishable by law.

118 The PC was amended in 2019 to better tackle technology-enabled sexual offences. This includes: (a) criminalising an entire spectrum of activities pertaining to abuse material, from production to distribution and possession of such material; [53] (b) sexual communication with minors; [54] (c) voyeurism and the

---

[53] s. 377BG – s. 377BL Penal Code.

[54] s. 376EA – s376EE Penal Code. Such offences cover communications that take place online and it is immaterial whether the communication originated in Singapore, as long as either the victim or the offender was in Singapore at the time of the communication.

distribution of voyeuristic images or recordings;[55] (d) the distribution of and the threat to distribute intimate images or recordings (also known as "revenge porn");[56] and (e) exposing one's genitals to another without that other's consent (also known as "cyber-flashing").[57]

119 POHA, which was enacted in 2014, contains a range of criminal measures to protect victims against offences involving harassment and abuse, both online and offline. POHA covers instances where a person causes the victim harassment, alarm or distress through any threatening, abusive or insulting words, behaviour or communications. Depending on the facts, sexual harassment, which would include intimate image abuse, may amount to harassment under POHA. POHA was also amended in 2019 to further protect victims by criminalising doxxing.[58]

---

55 Sections 377BB –377BD Penal Code.

56 Section 377BE Penal Code.

57 Section 377BF Penal Code.

58 Doxxing is made out if a person published personally identifiable information (e.g., photographs, contact numbers, addresses or employment details) of the victim, with (a) the intention of causing harassment, alarm or distress to another person; or (b) with the intent to cause the victim to believe unlawful violence would be used or to facilitate the use of unlawful violence, or knowing/having reasonable cause to believe that it would be likely to have these effects.

2. Regulatory measures

120 Beyond criminal law, new legislation was recently enacted to secure the online space, namely, the Online Safety (Miscellaneous Amendments) Act in 2022 (the "**OS(MA)A**"), and the Online Criminal Harms Act in 2023 ("**OCHA**").

(a) The OS(MA)A amends the Broadcasting Act 1994 to empower IMDA to issue directions to disable access by Singapore users to egregious content (e.g. posts advocating suicide, self-harm and terrorism) found on Online Communication Services ("**OCSs**"), which include social media services. OCSs with significant reach or impact in Singapore are designated and required, via Codes of Practice, to put in place measures to keep Singaporeans safe on their platforms.[59]

(b) The OCHA allows government directions to be issued in respect of online content or activity which is criminal in nature, with special provisions for online scams and malicious cyber activities.

121 As Minister Shanmugam noted in his opening remarks, these new legislative moves focus on what the State can do to deal with online harms, to

---

[59] IMDA issued the Code of Practice for Online Safety – Social Media Services in July 2023 to require designated social media services to have systems or processes in place to minimise Singapore users' exposure to harmful content, with additional protection for children.

protect our society. (Then) Judicial Commissioner Goh Yihan[60] recognised that these are *regulatory remedies*, that should be juxtaposed against *civil remedies*—a point which we will return to below.

3. Civil remedies

122 In contrast to the comprehensive slate of regulatory measures and criminal offences, civil remedies which vindicate the interests of persons affected by online harms emerged as a relatively weak point.

123 The importance of civil remedies cannot be gainsaid. Goh JC noted that:

(a) Civil remedies shift the focus from punishing criminal behaviour to vindicating the claimant's personal interests.

(b) The claimant may obtain a more direct and personal remedy, i.e., damages or an injunction. This is sometimes more useful to the claimant, as opposed to a fine or term of imprisonment imposed on the defendant.

(c) The standard of proof in civil claims is lower than in criminal proceedings.

---

[60] Judicial Commissioner Goh Yihan was appointed Judge of the Supreme Court on 1 October 2023. He was formerly a Professor of Law and the Dean of the YPHSL.

(d) While private prosecutions may be available to victims, such prosecutions are limited to selected criminal offences. In contrast, the existing common law causes of action arguably cover a broader range of wrongful conduct.

124 In this regard, Goh JC examined the existing common law causes of action which might be applicable to online harms. Goh JC noted that while the law of torts has evolved, the advancement of technology has confronted people with a wide range of digital actions that were never anticipated by early tort law. Surveying a range of torts—that of battery, the tort in *Wilkinson v Downton*, private nuisance and breach of confidence—Goh JC explained that each tort, as a result of its offline provenance, has limitations that render them ill-suited for addressing online harms .

125 Apart from the above, Goh JC observed that the statutory tort of harassment now embodied in POHA affords broader protection to a victim of online harms. In this regard, it is noted that POHA provides a range of civil remedies (e.g. damages, protection orders) to protect victims against harassment and related anti-social behaviour, as well as falsehoods. Pertinently, a new Protection from Harassment Court has been established, with simplified and streamlined court procedures to make it easier and cheaper for victims to apply for protection orders and expedited protection orders.

126 However, POHA is not without its limitations insofar as online harms are concerned:

(a) Goh JC noted that because POHA was conceived in relation to harassment, some have argued that there are a few situations which may fall outside of POHA—e.g. it has been suggested that ss 3, 4 and 7 of POHA may not be triggered if a victim discovers that a person has taken photographs of the victim on a single occasion, intending to keep them for personal gratification without publishing them.[61]

(b) Ms Simran Toor highlighted the practical constraints of POHA. In her experience, people find it challenging to navigate the Court process to obtain the remedies they are seeking; they would prefer a process that is simpler and faster.

(c) Mr Ramesh Selvaraj, in considering the remedies for offending statements under POHA, noted that a victim would have to contend with issues of burden of proof, in that, he/she has to show on a balance of probabilities that the offending statement is false. Moreover, POHA does not provide recourse where the offending statement made online is

---

[61] Singapore Academy of Law Law Reform Committee, Report on Civil Liability for Misuse of Private Information (December 2020) (Chairperson: Jack Tsen-Ta Lee) at 22.

factually correct or is an opinion, even if the said statement disproportionately affects one's reputation.

(d) Associate Professor Eugene Tan proposed creating new statutory torts for various online harms to enable victims to seek damages from wrongdoers in court.

127 In our view, civil remedies are the area most ripe for reform to better address online harms. We expand on this in the next section.

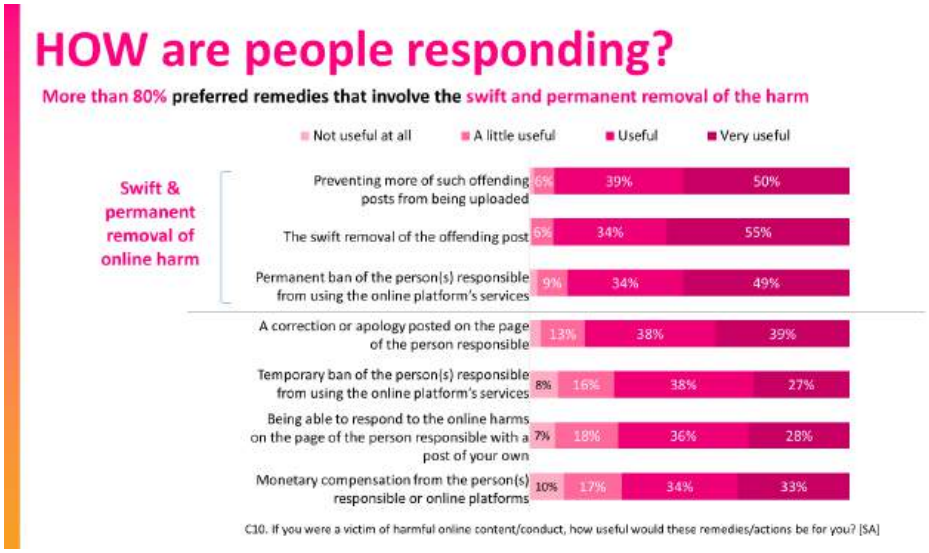
VII. NEEDS AND POSSIBLE SOLUTIONS

128 If civil remedies are a relative weak point in Singapore's suite of measures to address online harms, can anything be done to enhance the effectiveness of civil remedies? In this section, we set out some of the current difficulties with addressing online harms and our recommendations for how they can better be addressed.

A. Securing the expeditious removal of online harms

129 First, there is a need to provide victims with means to secure expeditious removal of online harms.

130 The SHE survey revealed that more than 80% of respondents preferred remedies that involve the swift and permanent removal of the harm. This includes the swift removal of the offending post, preventing more of such offending posts from being uploaded, and permanent bans of the persons responsible from using the online platform's services.



Credit: SG Her Empowerment.

131 This finding is not surprising. Whatever remedies may be available after the fact, long-term damage will already have been done if the online harm is not quickly removed.

132 However, under current legal frameworks, there is no certainty that a victim will be able to secure the swift removal of existing online harms, let alone the prevention of further harms.

133 Mr Ben Chua[62] shared that when CyberYouth Singapore ("**CYS**") conducts outreach activities with secondary school students, it recommends that they

---

62 President and Chief Executive Officer of Cyber Youth Singapore, a registered charity focused on empowering youths with skills and opportunities to become trailblazers of the digital future.

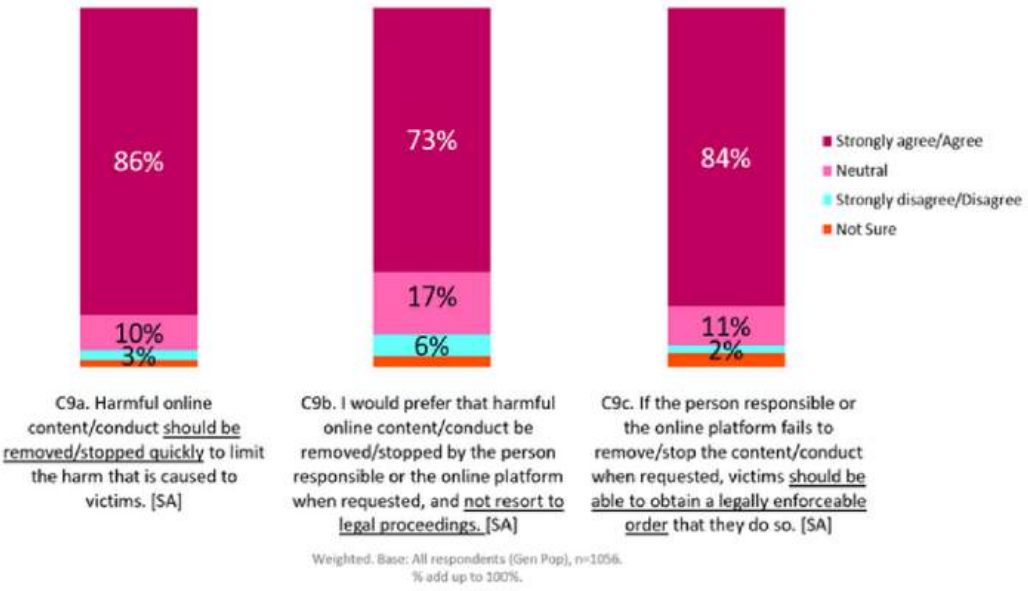
report online harms to tech platforms. Unfortunately, the feedback CYS often receives is that tech companies usually do not respond to such reports or follow up with any action. In Mr Chua's view, this indicates that the trust between the user and the platform no longer exists. Mr Chua added that it is very difficult to obtain any recourse from platforms, as there is no transparency in the reporting process and no certainty as to whether the platform will respond.

134 Ms Inman Grant observed that platforms are not perfect when it comes to addressing online abuse. Platforms have to address large numbers of reports and in doing so can miss context and culture. They also apply their own standards and practices unevenly. Ms Yuen Thio added that this is compounded by the fact that different platforms have different rules, which means that victims will have to navigate different regimes when harms take place across platforms. Ms Inman Grant shared the story of Gina, who had escaped an abusive relationship and started a new life with a new identity in a new town with her young son. Her violent ex-partner had just been released from jail, and her ex-partner's mother used Facebook to crowd-source and locate Gina so that her son could see his own son again. Ms Inman Grant added that despite the potential danger to Gina and her son, Facebook refused to remove the posts because they did not violate their terms of service.

135 In Singapore, such actions could arguably amount to unlawful stalking under POHA. If so, the Online Criminal Harms Act 2023 would provide assistance, as the competent authority appointed under that Act would be empowered to order the takedown of such posts. But one is left to wonder whether the criminal justice system must be engaged before action is taken. After all, the motivations of Gina's ex-partner's mother are understandable, and a person in Gina's position might not want to trigger criminal investigations and, possibly, prosecution.

136 Of greater concern is the fact that platforms may not act even when indisputably harmful and serious content is brought to their attention. Ms Inman Grant shared that the eSafety Commissioner and the Canadian Centre for Child Protection had in 2021 identified accounts on a social media platform involving necrophilia and bestiality and more than 120,000 connections to child paedophile networks. At the time, the eSafety Commissioner did not have the powers to order the removal of such content. When the company's Head of Trust and Safety was notified of this content and told that survivors of child sexual abuse had been reporting their own abuse on the platform, the response was that the content must have been reported incorrectly. In our view, this response does not speak well of the social responsibility of tech companies. A system that depends on users making reports "correctly" is perhaps not robust enough.

137 It is evident, then, that platforms, on receiving user reports, do not necessarily take prompt action to address online harms. Would a legal process provide a better recourse for victims? For victims of online harms, this appears to be a last resort. 73% of respondents to the SHE Survey indicated that they would prefer that the harmful online content / conduct be stopped by the person responsible or the online platform when requested, without having to resort to legal proceedings.



Credit: SG Her Empowerment.

138 Again, this finding is not surprising. Commencing legal proceedings generally requires a litigant to engage a lawyer and to contend with court processes, which will entail time and money. Court proceedings are therefore

unappealing to victims who are further deterred by the uncertainty over the likely outcome that is part and parcel of an adversarial process.

139 Moreover, the court process may compound the distress suffered by victims. Ms Inman Grant shared that when image-based abuse cases go to court, female victims are often forced to share in the courtroom the intimate imagery that caused them so much torment, when victims simply want the images taken down without having to relive the trauma in court proceedings. Ms Simran Toor shared that even when the court process is designed for claimants to take action without a lawyer, they still prefer something that is faster and simpler. Even when victims evince the intention to go ahead with POHA proceedings, they may not follow through because there are too many follow-up steps that need to be taken and people fall by the wayside. This was the case for Eve, who reported finding it "overwhelming" to attempt to file a POHA application on her own.

140 In considering reform under Singapore law, it may be helpful to refer to the measures put in place by the Australian eSafety Commissioner to secure the removal of online harms without having to resort to legal proceedings. Ms Inman Grant explained that eSafety functions as a "safety net" when platforms fail to act on reports of abuse and ability to bridge the "inherent power balance that exists between tech behemoths and the users who often don't have any recourse".

141 eSafety administers complaints schemes for four categories of online harms, receiving complaints from the public and securing the expeditious removal of actionable online harms with an admirable success rate of more than 80% for actionable child cyberbullying, adult cyber abuse and image-based abuse.[63] eSafety generally manages to secure the removal of harmful online content within 24 hours, and has managed to have some content taken down within 12 minutes.

142 Ms Yuen Thio endorsed establishing an independent agency with powers that enable them to swiftly act against online harms, because what most survivors of online harms want is the ability to have almost immediate action. She added that going through a normal government agency or the court system would be the same as getting no redress, because these processes would not be able to provide this remedy. Likewise, Ms Simran Toor noted the disjunct between the number of people reaching out for help and of those seeking recourse, due to the roadblocks and challenges encountered by the latter group. She stressed that we cannot end up with a situation where victims are unable to seek remedies and recourse and perpetrators get away scot-free. She suggested that an innovative means of addressing the issue such as the powers entrusted to the eSafety Commissioner would be a great idea.

---

[63] Annual Report 2022-23, Australian Communications and Media Authority and eSafety Commissioner, page 201.

143 Ms Simran Toor shared that harassers do not just perpetrate their harms via a single platform. Instead, since the intent is to overwhelm, they do so by stalking and defaming the victim over multiple platforms and messaging services. Therefore, harassers blocked on one account can just pop up using a different account or on a different platform. The agency should have the power to address online harms affecting a victim across multiple platforms.

144 Crucially, such an agency must have bite: that is, the orders they issue must be enforceable and their breaches punishable. Ms Inman Grant shared that she did not think that eSafety would have had the same degree of success with platforms if they did not have powers to impose fines and other remedial powers. These powers are significant. Under the Australian Online Safety Act 2021, end-

users and social media platforms which fail to comply with a removal notice face a civil penalty of up to A$156,500 and A$782,500 respectively.[64]

145 However, the agency must be able to exercise flexibility and discretion in its handling of each case of online harm. Ms Inman Grant gave an example of a 14-year-old girl subject to cyberbullying by six of her peers. While the cyberbullying was undoubtedly very serious, involving rape and death threats, eSafety worked with the parents of the perpetrators to force them to take down the harmful content and write letters of apology, rather than to fine them.

146 Finally, given the global nature of the internet and the fact that online harms perpetrated anywhere in the world can impact people in Singapore, it is imperative that such an agency is able to act effectively to address online harms originating overseas.

147 Ms Julie Inman Grant noted that many rogue sites are set up in permissive hosting environments overseas and that it is easy for bad content hosts to move between jurisdictions. Indeed, most, if not all, of the online harms which her agency deals with are hosted outside of Australia. The same is likely to be true of online harms that affect Singaporeans.

---

[64] Sections 67, 80, 91, 111, 116 Online Safety Act 2021.

148 It is therefore appropriate that the Australian Online Safety Act 2021, pursuant to which the eSafety Commissioner is established, is expressly stated to extend to "acts, omissions, matters and things outside Australia".[65] As a consequence, the eSafety Commissioner has been extremely successful in securing the removal of online harms within its remit. In the case of child sexual exploitation material, their success rate is a remarkable 90%. This underscores the need for legislation in Singapore to be similarly expansive, and to have effective measures of enforcement against parties overseas who ought to be held accountable.

Recommendations:

- **To provide victims of online harms with an accessible way of swiftly and permanently removing harmful online content.**

- **Taking eSafety's example, this could be done through an agency empowered to receive complaints regarding online harms and to issue legally enforceable directions to address those complaints.**

---

[65] Section 23 of the Australian Online Safety Act 2021.

- **Empowering the agency to act flexibly in appropriate circumstances. For example, this could entail referring complaints to other parties better placed to address the issue. This could include community partners, counsellors schools, or other authorities such as the Police.**

B. Improving the ecosystem of accountability

149 Second, there is a need to improve the ecosystem of accountability. This entails holding those responsible for online harms accountable and allowing victims of online harms to obtain redress when they are affected. This is a concept that is familiar to all lawyers, as it is central to the law of torts.[66] As Goh JC explained, civil claims are important because they, among other things, vindicate a claimant's personal interests and provide a more direct and personal remedy in the form of damages or an injunction.

---

[66] See Tort Theories in "*The Law of Torts in Singapore*", Gary Chan Kok Yew and Lee Pey Woan, Academy Publishing, Second Edition, 2011 at 01.025-01.056.

150 However, while the merits of civil claims are clear, they suffer from a number of disadvantages which Goh JC outlined in his remarks:

(a) Potential claimants may be unable to afford to hire a lawyer and may be unwilling to endure additional unwanted publicity.

(b) Monetary damages may be difficult to collect and injunctive orders may be difficult to enforce, particularly in cross-border cases.

(c) Existing common law causes of action were developed incrementally in the past to redress physical harms so they may not squarely address online harms.

151 Thus, drawing inspiration from the statutory tort of harassment created under POHA, Goh JC suggested that it may be better to have focused legislation

that is targeted at online harms, with Parliament uniquely placed to take a root and branch approach as to the appropriate action to empower victims and provide them with swift and accessible solutions.

152 We agree with these observations. A root and branch approach will entail having regard to the realities of online harms. One key consideration is the damage that is suffered by victims. As noted above at paragraph 58 above, the most common consequence of online harms reported by respondents of the SHE Survey was feeling angry, sad, anxious, embarrassed, ashamed or helpless. It is trite law that there is generally no liability for causing emotional distress. In this regard, Goh JC highlighted that many victims of online harms suffer annoyance, embarrassment or distress that is serious but do not amount to an actionable psychiatric illness. However, given that emotional distress is the usual damage suffered by victims of online harms, it is important to consider whether emotional distress ought to be specifically recognised as a recoverable loss in the context of online harms.

153 Moreover, there should be clarity about the parties to be held accountable under the statutory tort. In this connection, it is reasonably clear that those who perpetrate online harms or who would be considered joint tortfeasors under existing law should be included.

154 The more contentious issue concerns whether tech companies should be held liable in some way for online harms taking place on their platforms. There is a growing consensus that these companies are important partners, and have important responsibilities, in keeping the internet safe.

155 Ms Haugen observed that we are missing an ecosystem of accountability when it comes to social media because of an information asymmetry between social media companies and everyone else.

156 Taking automotive safety as an example, Ms Haugen described the ecosystem of accountability that has led to a remarkable decrease in the fatality rate from motor vehicles in the United States since 1965. This ecosystem included regulation, informed legislators, investors prioritising long term returns over short term returns, and concerned citizens. More pertinently for the present discussion, it also included class action litigation to push things towards the common good.

> *"… when we think about online regulation, the central piece of that is recognising that we are seeking to hold businesses liable for the systems they've created to make money for themselves, and we do that in every other industry and there is no reason why we should not do it in technology as well."*
>
> - Mr Damian Collins, MP

157 In our view, litigation, whether class action or otherwise, is pivotal for improving accountability of tech companies. This point is illustrated by the state of affairs that arises when it is removed from the ecosystem of accountability. This has happened in the United States, as a result of the introduction of section 230 of the Communications Decency Act of 1996.

158 While section 230 was introduced with the intention of incentivising private efforts to combat offensive material, the US Courts have interpreted the

provision differently.[67] Professor Danielle Citron has observed that section 230 has been interpreted to provide shields against liability for diverse bad actors such as sites that deliberately republish illegal content, sites that solicit users to engage in tortious or otherwise illegal activity, and sites that enhance the visibility of illegal activity while ensuring that perpetrators could not be identified and caught. In Professor Citron's view, the provision as interpreted by the courts provides a free pass for tech companies to maintain and not take down content containing destructive, criminal and tortious activity despite being apprised of it. It is for this reason that the United States has more than 9,000 sites devoted to non-consensual intimate imagery.

> "*A brick-and-mortar business that makes it easy for third parties to stalk and invade the privacy of victims faces tort liability for enabling the abuse. A hard-copy magazine that published user-submitted non-consensual porn encounters a blizzard of privacy lawsuits. But when those activities happen online, companies are shieled from liability. We have Section 230 of the Communications Decency Act to thank for that.*"
>
> - Professor Danielle Keats Citron[68]

---

67 See *The Fight for Privacy: Protecting Dignity, Identity and Love in the Digital Age*, Danielle Keats Citron, W W Norton & Company, First Edition 2022, at pp 84-90.

68 *The Fight for Privacy: Protecting Dignity, Identity and Love in the Digital Age*, Danielle Keats Citron, W W Norton & Company, First Edition 2022, at p 84.

159 Speaking from a litigator's perspective, Mr Adam Massey noted that as a result of section 230, it is cheaper for a tech company to deal with an American plaintiff by hiring a lawyer to argue that a case should be dismissed than building meaningful trust and safety for their users.

160 It should be noted that section 230 is not only a concern for people in the US. In this regard, we can do no better than to quote Professor Citron:[69]

> The lack of geographic borders online gives Section 230 an outsized impact. When non-US sites remove non-consensual intimate images, perpetrators do the next best thing—they post the images on US sites. The images will likely remain up, no matter how much victims complain. In short, perpetrators can always torment victims on sites hosted in the United States, and victims' home countries can't do anything about it.
>
> …
>
> It doesn't have to be this way. In the EU, sites can face liability for third-party content if they receive notice and fail to expeditiously remove the content. In Germany, under the Network Enforcement Act of 2018, social media companies with more than two million subscribers must remove "clearly illegal" content within 24 hours of receiving a complaint. In the United Kingdom, sites are shielded from defamation liability only if they follow a notice-and-takedown procedure set forth in the Defamation Regulations of 2023.

---

69 *The Fight for Privacy: Protecting Dignity, Identity and Love in the Digital Age*, Danielle Keats Citron, W W Norton & Company, First Edition 2022, at p 89.

161 In our view, this behoves all countries, including Singapore, to determine for themselves when tech companies should be liable for content posted on their platforms.

162 Tech companies may well disagree that more needs to be done, or disagree with the possible solutions put forward. Building on Ms Haugen's example of automotive safety, Ms Inman Grant observed that car manufacturers had pushed back on having to invest heavily in safety in the past, but today many safety features in cars have come to be taken for granted, with safety by design a guiding manufacturing principle and car manufacturers competing on safety features. Ms Inman Grant observed that the technology industry needs to have their seat belt moment. Whilst the process of reform ought to involve consultation with tech companies, their views and interests should not trump those of victims of online harms and society at large.

Recommendations:

- **Consider introducing statutory torts to provide clarity and certainty on the causes of action that victims of online harms can pursue to obtain redress.**

- **Consider whether emotional distress should be recognised as a recoverable loss in the context of online harms.**

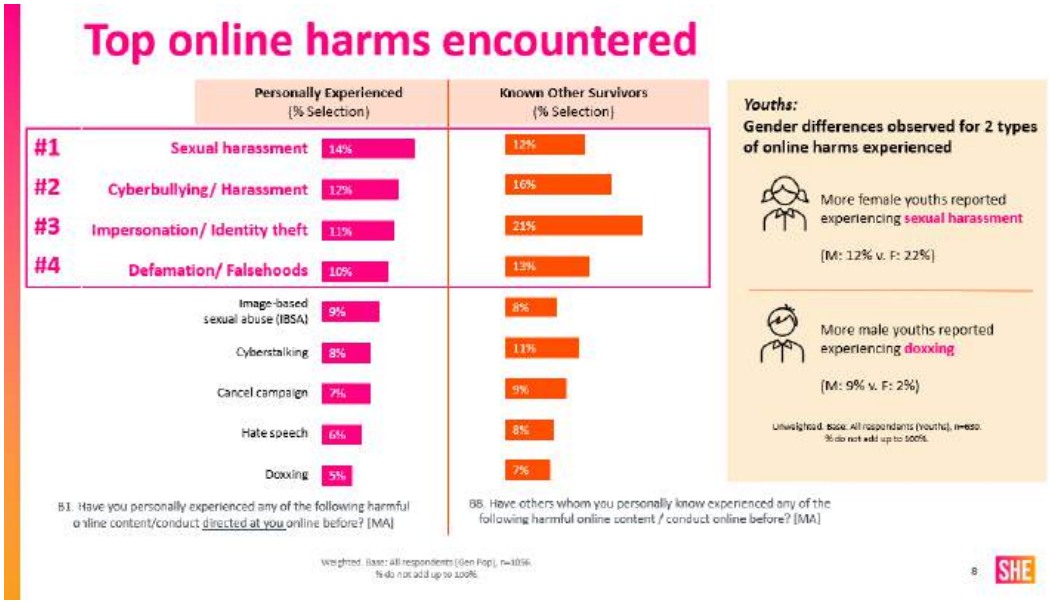
- **Ensure that all parties responsible for online harms can be held accountable. This should include identifying appropriate circumstances in which tech companies should be liable for online harms that take place on their platforms.**

C. Identifying appropriate categories of online harms to be addressed

163 We have discussed the need for the swift and permanent removal of online harms and improving the ecosystem of accountability for online harms. But what does the label "online harms" refer to and *which* online harms ought to be addressed? In this regard, we agree with Ms Toor's observation that the term is a nebulous one and there is a need to define more clearly what online harms are.

164 We agree with Ms Yuen Thio that as a starting point, this important task of defining "online harms" cannot be left to the policies of tech companies because community standards differ between platforms. More fundamentally, we agree with Mr Collins' view that the terms of service and community standards set by platforms should not be the last word, and that there must be a minimum safety standard that we would regard as being acceptable in our own laws. Equally important is the signalling effect that the law has, when something is described by the law as an online harm.

165 More concretely, the forms of online harms studied in the SHE survey is a good starting point.



Credit: SG Her Empowerment.

166 In addition to accurately identifying and thereby remedying existing forms of online harms, it is also important to put in place mechanisms to swiftly respond to new and emerging types of harms.

167 This need is demonstrated by the history of the eSafety Commissioner, whose remit has grown over the years as the need to address other forms of online harms becomes apparent and urgent. It began as the Children's eSafety Commissioner in 2015 before expanding to cover all Australians in January 2017. In October 2017, after an image board was set up to share the intimate images of

Australian school girls, eSafety launched an image-based abuse portal. In 2019, following the livestreaming of a shooting at a mosque in New Zealand, eSafety was given powers to tackle abhorrent violent content and conduct.

168 Indeed, it is difficult to predict future forms of online harms, given how the technology to perpetrate them may not exist today.

169 Professor Lim Sun Sun shared a recent example where AI-generated naked images of young girls from a Spanish town had circulated on social media without their knowledge.[70] These pictures were created using photos of the targeted girls fully clothed. Professor Lim observed that although generative AI had only entered the public consciousness in around November 2022, small communities are already being traumatised by it, and it would become even easier for such manipulation to be undertaken by anyone. Likewise, Ms Julie Inman Grant noted that the eSafety Commissioner has started to receive reports of AI-generated abuse. Since then, the scale of the problem has been brought home to the public consciousness when such images of Taylor Swift flooded X.[71]

---

70 "*AI-generated naked child images shock Spanish town of Almendrakejo*", BBC, 23 September 2023.

71 "*Explicit deepfake images of Taylor Swift elude safeguards and swamp social media*" New York Times, 26 January 2024.

170 Looking beyond the horizon, Ms Inman Grant noted that with the Metaverse and immersive technologies such as Oculus glasses and full haptic suits, harassment will feel like sexual assault – hyper realistic, harsh, high impact and very visceral.

171 Where possible, legislation should be drafted in a manner which allows emergent forms of online harms to be addressed, even if they are not a significant problem at the time the law is passed or could not have been foreseen. This could involve the use of definitions with some degree of in-built elasticity to capture new forms of harm, bearing in mind always the need for legislation to be precise, or legislation which can respond to changing circumstances (e.g. through subsidiary legislation or codes). Otherwise, regulators and the authorities would often have to play catch-up.

172 It is apposite to return to Mr Woon's presentation. While his remarks were directed at cancel culture, they are also relevant in emphasising the importance of precisely identifying online harms in order to address them through the law. Mr Woon had cautioned that no one can really define Cancel Culture satisfactorily, observing that it is still an evolving phenomenon and not something that is susceptible to precise definition. Having said that, he opined that it was not necessary to define "cancel culture", and that a definition that is good enough for us to respond to would suffice. In his view, it is practicable and actionable to

identify activities associated with cancel culture that are wrongful and that need to be addressed. This is sensible and, indeed, is commonplace in legislation. For example, the term "harassment" is vague, yet POHA addresses such conduct by defining the objectionable behaviours with precision.[72]

173 Given the relative recent emergence of cancel culture in the public consciousness and the imprecision of the term, it is worth dwelling further on Mr Woon's remarks. In this regard, Mr Woon identified four broad categories of "cancellation" differentiated by the motivation of the perpetrator:

(a) Category 1: seeking accountability.

(b) Category 2: seeking justice.

(c) Category 3: seeking to censor.

(d) Category 4: seeking to inflict harm.

---

[72] See sections 3 – 7 of POHA.

174 In Mr Woon's view, drawing the line between acceptable and unacceptable behaviour involves distinguishing between constructive and destructive uses of freedom of speech. In that light, the first two categories are probably legitimate uses of freedom of speech, while the latter two are not. Indeed, Mr Woon argues that the Government has a legal and moral duty to ensure that its citizens are able to substantively exercise the right of freedom of speech, free from undue influence, while balancing this against contravening the right of the would-be canceller to freedom of speech by intervening.[73]

---

[73] "*Cancel Culture and Freedom of Speech: Definitions, Effects, and the Way Forward*", Alexander Joseph Woon.

Recommendations:

- **To identify and clearly define what online harms are to be addressed, taking care to isolate wrongful behaviours rather than to rely on labels.**

- **To ensure that emergent forms of online harms and changing circumstances can be addressed in a timely way.**

D. Protecting reputations online

175 We turn next to the issue of reputational harms on the internet.

176 Professor Ardia has observed that the internet has profoundly altered the way that people create, disseminate and use reputational information. It has made reputation more enduring yet more ephemeral – enduring because information about us whether good or bad can exist and be easily retrieved forever; ephemeral because a person's reputation is open to onslaughts from many more sources. As a result, the traditional approach of sending a cease-and-desist letter or demanding a retraction no longer accomplishes its purpose. Professor Ardia elaborated:

> Our existing notions of how to establish trust and maintain social ties do not always translate to this networked world, and as a result

> traditional approaches to protecting reputation that were blunt and ineffective, even before the internet, are even less effective today. The legal doctrines that deal with reputational harm simply have not kept up with these changes. The heterogenous networked society that we know today is far different from the feudal system that predominated during the 13th century when the law of slander got its start, or even the more enlightened 17th century when the Court of Star Chamber developed the common law of libel in response to the printing press. While the way we use reputation has evolved and is still evolving, along with our communication, political, and social systems, defamation law remains distressingly out of step with our increasingly networked society.

177 Mr Selvaraj agreed, noting that the digital landscape has transformed the way that reputation can be damaged, with offending material going viral very quickly, reaching a large audience and thus causing great and lasting harm. Speaking from a practitioner's viewpoint, he explained that many clients may not have the time, resources and patience to go through the court process and do not desire the remedies offered by defamation litigation.

178 Elaborating, Mr Selvaraj explained that defamation cases are never open and shut with the court having to hear arguments on both sides and determining the meaning of the offending statements. Therefore, even if judgment is obtained in the victim's favour, it often comes too slow in comparison to the harm that has been occasioned. He gave the example of a client who had been accused online of being an adulterer: within two hours, the post had been shared repeatedly on Facebook and circulated on WhatsApp.

179 Further, even if a defamation claim succeeds, the usual remedy that is awarded is monetary compensation. In Mr Selvaraj's view, this is not an intuitive remedy as it does not truly vindicate a victim's reputation, a point supported by Professor Ardia. While a judgment may be delivered, this may not do the victim any good if it is not read or seen by the individuals who have seen the defamatory statements.

180 Going further, Mr Selvaraj noted that there may well be instances where what is said online may be factually correct but objectionable (for example, it is taken out of context) and can disproportionately affect one's reputation. These would not be covered by the tort of defamation or the framework for addressing false statements under POHA, and Mr Selvaraj opined that this is a gap that needs filling.

181 Under the common law, the defence of justification is available for a defamatory but truthful statement, on the basis that the subject's reputation is not lowered beyond its proper level.[74] Further, the defence of fair comment is available for comments based on true facts, to protect the right of free speech and to promote open discussion.[75] These defences are longstanding and have sound justifications. In our view, it would surely be inappropriate for damages to be awarded for truthful statements or opinions.

182 However, much of the law of defamation developed before the internet allowed reputations to be affected in such profound and lasting ways. Moreover, it is premised on the court making a finding of fact on a balance of probabilities through an adversarial process and the primary remedy being compensatory damages. We agree with Justice Philip Jeyaretnam's[76] view that court-based remedies are necessary but not sufficient, and that the modes of seeking redress must be reformed and adapted in every generation. In this regard, Jeyaretnam J observed that an integral part of access to justice is in ensuring that ordinary individuals can remedy harms in a way that is quick and affordable, and that

---

74 "*The Law of Torts in Singapore*", Gary Chan Kok Yew and Lee Pey Woan, Academy Publishing, Second Edition, 2011 at 13.004.

75 *Ibid* at 13.012.

76 Justice Philip Jeyaretnam is a Judge of the Supreme Court of Singapore. He has been the President of the Singapore International Commercial Court since 2 January 2023, and is a member of both the Judicial Service Commission and Presidential Council for Minority Rights.

processes that achieve good-enough outcomes, quickly and at reasonable cost, are important.

183 Mr Selvaraj gave an example of one such good-enough outcome, noting that a client may just want to have an opportunity to have his voice heard by providing context or a rebuttal to the offending statement. This was the case for his client who was accused of adultery, who had wanted an opportunity to respond to the offending post in a manner which would reach the same audience. In a similar vein, Professor Ardia proposed that the focus should be on ensuring the reliability of reputational information rather than imposing liability. Giving a claimant the opportunity to respond to an offending statement builds greater capacity to assess the veracity of speech and to contextualise it. Additionally, Professor Ardia emphasised the value of such a remedy being embedded in the networks and communities people are in – people will readily be able to provide notice of defamatory speech and have an opportunity to be heard. In his view, this would deter and prevent defamatory speech because potential defamers know that they will not get away with it.

184 Such a remedy may not require lengthy court proceedings, with its adversarial and forensic processes. Jeyaretnam J noted that the safeguards of the burden of proof and the processes surrounding it are appropriate for a remedy such as damages. However, where a less onerous remedy such as a right of reply

is concerned, particularly in an online context with no limitations on space such as in a traditional reply, then the remedy could be granted much more readily without necessarily coming to a final view of the veracity of the statement. Mr Selvaraj agreed, musing whether the neatest remedy would be an opportunity to respond to allegations as quickly as possible. Such a reply need not be granted by an adjudicatory body, and could instead be screened for proportionality, which he described as a very low bar. Ideally, the reply would be tagged to the original offending statement, so that any inequality between the parties is balanced out.

185 To this, we would stress that such a reply must also be swift. As Professor Ardia has noted, the quicker we can engage these processes the better, as the longer a defamatory falsehood goes unchallenged the more likely it is to cause reputational harm.

186 It should be noted that protecting reputation is not only about protecting the individuals whose reputations have been affected. In Professor Ardia's view, reputation is in many ways a quintessential public good which serves an important signalling function by communicating complex information about the individual and his/her place in society. When an individual's reputation is improperly maligned, it degrades the value and reliability of this information and devalues community identity.

Recommendations:

- **Consider new measures for protecting reputation online, premised on providing an aggrieved party with a means to respond to an offending statement swiftly and effectively.**

E. Addressing online anonymity

187 We turn next to online anonymity. Two issues emerged during the Symposium.

188 First, while there are existing legal processes to identify a perpetrator, these are not readily accessible to victims. Associate Professor Eugene Tan shared that while the Court has the jurisdiction to grant pre-action discovery (*i.e.* the power to order production of documents and information that is needed before the commencement of any legal proceedings), this entails commencing court proceedings with the associated legal fees and time required, and this procedure is only available for the limited purpose of commencing legal proceedings. Associate Professor Tan argued that more legal support should be provided to victims of online harms, including avenues for self-help that are accessible, quick, and cost-effective.

189 With reference to the US context, Mr Adam Massey shared that obtaining information regarding the identity of perpetrators requires litigants or their counsel to send out subpoenas to tech companies, which have 30 days to respond. However, tech companies are likely to fight such subpoenas, and the process could take more than 90 days. If tech companies take the same approach to pre-action discovery in Singapore, victims can expect their applications to be contested, adding to the legal fees, delay and uncertainty.

190 Second and more importantly, these legal processes may not even be effective. Mr Ben Chua explained how easy it is for one to remain anonymous online. Some platforms encourage anonymity by not requiring users to identify themselves when registering with the platform. While others do collect more information, it is possible to bypass these requirements using readily available tools such as virtual private networks or TOR browsers. This was borne out by Mr Massey's experience. He shared that when a tech company does respond to a subpoena, the victim may be supplied with limited and unhelpful information: a fake email address and an IP address masked by a VPN. A victim could then try to subpoena the VPN provider but VPN providers do not know the identity of the perpetrator by design because they compete on storing the least amount of information.

191 In Mr Massey's view, the odds are stacked against victims even when they are able to afford legal representation, because of platforms' wilful refusal to store enough records about who is behind this bad conduct. Indeed, even the eSafety Commissioner encounters the same practical challenge, in spite of it being statutorily empowered to obtain from platforms information about the identity of its users.[77] While this is a powerful tool to help eSafety conduct investigations and identify the person behind the account so that it can issue notices to that person, Ms Inman Grant shared that many platforms collect very little information when users sign up, and it is therefore very easy for users to remain anonymous online.

192 The end result, as observed by Associate Professor Tan, is that victims often have to act like private investigators to uncover the real identities of perpetrators. He cautioned against normalising online harms through inaction. Moreover, even as we seek to derive benefit from the online world, we must do what is necessary and right to mitigate the harms and right the wrongs.

---

[77] Section 194, Australian Online Safety Act 2021.

193 Associate Professor Eugene Tan and Dr Tracy Loh both called for increased traceability of internet users as a way of addressing online harms. Associate Professor Tan explained that this was really a call for more responsibility and accountability of all stakeholders with regard to the internet, opining that the expectations of people should not differ just because they are on the internet. Associate Professor Tan added that it is vital to have the online space characterised by responsible and accountable behaviour by all relevant stakeholders. Where platforms fail to remove or put a stop to, or even enable online harms, despite their being informed of them, then they should be held accountable. Separately, Professor Lim Sun Sun commented that if we can create a situation where people are not able to get away with their online actions so easily, they would take much more responsibility for their actions.

194 In our view, consideration should be given to requiring platforms to collect more information from users to ensure they can be traced and identified in the event that they perpetuate online harms.

Recommendations:

- **Consider alternatives to pre-action discovery to allow victims to identify perpetrators of online harms.**

- **Consider requiring tech companies to obtain more information from users to ensure that they can be traced and identified in the event that they perpetrate online harms.**

F. Other measures

195 Finally, it should be emphasised that laws and legal remedies are not a silver bullet solution to online harms. Educating Singaporeans on digital literacy, promoting community organisations that support victims of online harms, and facilitating cross-sector collaborations to encourage conversations about online safety, are amongst the many ground-up and Government initiatives that help to create a safer online space for our society.

196 For example, Professor Lim Sun Sun shared her experience with the Sunlight Alliance of Action, which developed various self-help resources on what people and bystanders can do to deal with online harms.

197 The support provided by initiatives such as SHECARES@SCWO is indispensable. Andrew shared that the counsellor at SHECARES@SCWO was always there to help and support him, providing a safe space and environment for him to express his feelings and concerns. He was of the view that he would probably still be drowning in anxiety if not for the support of SHECARES@SCWO.

198 There have also been efforts to strengthen digital literacy in Singapore, particularly amongst youth.

(a) MOE's National Digital Literacy Programme for schools and Institutes of Higher Learning focus on various digital competencies including digital safety and security – equipping students with the knowledge of how to protect oneself in the online space.

(b) The Media Literacy Council under the IMDA, which promotes cyberwellness, has developed useful resources to promote safe and responsible behaviour online.

199 MCI has also worked with technology companies to launch an Online Safety Digital Toolkit, which guides parents to make use of the parental controls,

privacy and reporting tools, as well as self-help resources on the social media platforms.

200 In our view, these are indispensable complements to criminal, regulatory and civil measures, and more efforts in these areas are to be welcomed.

201 It is also important to remember that, as users of the internet, all of us have a role to play in combatting online harms. As Dr William Wan[78] noted, if we were all kind – by graciously respecting the dignity of everyone, taking a listening and non-judgemental stance, and doing unto others as we would expect others to do to us – we would not be facing as many challenges in the area of online harms. Moreover, rather than being bystanders to online harms when they occur, we could intervene in a measured and respectful way by having a conversation with the person who is responsible for the online harm.

---

[78] General Secretary, Singapore Kindness Movement.

VIII. CONCLUSION

202 In opening the Symposium, Minister for Law K Shanmugam noted that recent legislation to address online harms have allowed the state to better regulate the online space. Looking forward, Minister Shanmugam emphasised the need for further laws to empower victims of online harms, rather than the state, to take action to protect themselves. Based on feedback from respondents to the SHE survey and other studies, he ventured the view that the top priority for victims would be to stop the online harm, through the swift and permanent removal of harmful online content. If possible, other remedies such as monetary compensation could be pursued.

203 As can be seen from this report, the discussions over the course of the Symposium certainly underlined the urgent need for legal intervention to empower victims of online harms. In delivering the closing address, Senior Parliamentary Secretary Rahayu Mahzam highlighted that there appeared to be consensus amongst the panelists that an ecosystem of accountability is long overdue, and that there is a need to re-look existing frameworks and infrastructure in the online space.

204 We are pleased to see that this has since developed into the launch of a public consultation by the Ministry of Law and Ministry of Digital Development and Information in November 2024. No doubt informed by the learnings from the Symposium, the proposals put forward for public consultation are aligned with the recommendations set out in this report.The YPHSL is glad to have contributed to this effort to address real world challenges by co-organising the Symposium.

Yong Pung How School of Law
55 Armenian St
Singapore 179943
https://law.smu.edu.sg law@smu.edu.sg

Copyright © 2025 Singapore Management University