ISSUES PAPER ON CYBER-HARASSMENT, CYBER VIOLENCE AND OTHER HARMFUL CYBER BEHAVIOUR

BACKGROUND AND ISSUES TO BE ADDRESSED

0.1 The growing use of information and communication technologies (ICT) has become a double-edged sword – on one hand, ICT significantly increased access to information and opportunities and has made communication faster and easier. On the other hand, ICT has brought about unfavourable consequences – it has been used as a tool to inflict harm on others; harm in this instance refers to cyber communications that are abusive, threatening or invasive of privacy.[1]

0.2 More and more reports of threats of violence, rape and killing have emerged in Malaysia – for example, a young woman (who was caught on video hitting the car of an elderly man after a motor vehicle accident) had her car registration number and other private information exposed and it went viral within 24 hours; a radio presenter received rape and death threats (when she asked on a YouTube video whether *hudud* law would be able to address the socio-economic issues in Kelantan); and a young man received thousands of death threats and other hateful messages when he organised a dog familiarisation event. This problem is not exclusive to Malaysia - according to the United Nations, 73 percent of women and girls have been exposed or have experienced some form of online violence.[2] In most of these cases, perpetrators of cyber threats/harassment are rarely held accountable for their behaviour and the possibility of being anonymous in cyber space exacerbates this problem.

0.3 Threats of rape, death and exposure of private data, information and photographs are emotionally stressful and the damage they inflict on their victims can sometimes extend to physical trauma. In turn, this results in a direct and indirect cost to society and the economy – the need for health care increases and resort to judicial and social services rises, in turn driving up financial resources and productivity decreases once peace and personal security of a person is threatened.[3]

---

[1] Issues Paper on Cyber-crime affecting personal safety, privacy and reputation including cyber-bullying' (LRC IP 6-2014, *Law Reform Commission*, <http://www.lawreform.ie/_fileupload/Issues%20Papers/ip6Cybercrime.pdf> accessed 24 March 2016.

[2] 'Cyber Violence Against Women and Girls – A World-Wide Wake-up Call', A Report by the UN Broadband Commission for Digital Development Working Group on Broadband and Gender, (2015), <http://www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf> accessed 24 March 2016.

[3] 'Cyber Violence Against Women and Girls – A World-Wide Wake-up Call', A Report by the UN Broadband Commission for Digital Development Working Group on Broadband and Gender, (2015), <http://www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf> accessed 24 March 2016.

Rationale for the Campaign

0.4 Malaysia has the fourth highest proportion of youth Internet usage worldwide,[4] and the use of ICT, including the Internet, will continue to grow exponentially, particularly, amongst the younger generation. As such, it is important that the Internet is made a safer, respectful and empowering space, for current and future generations.

0.5 To ensure this, the government, law makers, industry players and the general public must demand and act against the violence perpetrated in cyber space. As there are currently no specific laws that tackle cyber threats/harassment and other harmful cyber behaviour in Malaysia, it is therefore necessary to ascertain whether there is a need for relevant legal provisions to tackle this growing problem.

0.6 Legal reform on its own is insufficient – there must be public awareness on the problem to ensure that not only harmful cyber behaviour is called out but that cyber users are able to ensure that they behave in a respectful manner when using cyber technologies. Increased public awareness will also ensure that legal reform will have a wider impact.

Commitment to participatory democracy

0.7 With a firm commitment to the principle of participatory democracy, including an increase in effective participation of Malaysians in the legislative process, the PeopleACT believes that law reform could and should include meaningful consultation with stakeholders. As such, the PeopleACT would like to start the law reform portion of the PeopleACT campaign with this Issues Paper, which serves as a consultation document to obtain views and opinions from stakeholders on whether the current law in Malaysia is sufficient to tackle the problem of cyberharassment and other harmful cyber behaviour.

0.8 This Issues Papers reviews Malaysian legislation that is relevant to cyberharassment and other harmful cyber behaviour, in particular the Communications and Multimedia Act 1998, the Penal Code, and civil action such as, privacy and harassment. The Issues Paper also looks at laws in other jurisdictions, such as the United Kingdom (UK), Australia, Hong Kong, Ireland and the European Union (EU), to see how the laws in these jurisdictions deal with cyberharassment and other harmful cyber behaviour.

0.9 In addition, the Issues Paper draws upon a quantitative survey carried out by the PeopleACT from 8 June 2016 to 31 December 2016 (the "Survey"). The Survey conducted received 522 responses, of which 336 (64.4 percent) identified themselves as women; 183 (35.1 percent) identified themselves as men; and three respondents identified themselves as from the 'other' category.[5] Majority of respondents (52.1 percent) were 17 to 24 years of age and most respondents were from Selangor (52.7 percent) or Kuala Lumpur (23.8 percent). The Survey was targeted at Malaysians where 97.1 percent (i.e. 507 responses) identified themselves as Malaysian. See **Annex 1** for the report of the Survey.

0.10 Apart from the Survey, the Issues Paper will also refer to excerpts from 35 incidents conducted with victims/survivors of cyberharassment and other harmful cyber behaviour and incidents reported in the media. All interviews are anonymised to protect the confidentiality, safety, and security of the interviewees. Where possible, any reference to gender has been omitted/ randomised.

---

[4] 'Exploring the Digital Landscape in Malaysia', UNICEF (November 2014), 41 <http://www.unicef.org/malaysia/UNICEF_Digital_Landscape_in_Malaysia-FINAL-lowres.pdf> accessed 4 Mar 2016.

[5] 'Other' was an option given to recognise the possibility of a third gender identified by the respondents themselves.

0.11 At this juncture, the PeopleACT would like to state at the outset that it is committed to freedom of expression in accordance with international human rights standards i.e. that freedom of expression is the general rule. As it is not an absolute right, restrictions are permissible so far as it is provided by law (and interpreted narrowly); proportionate; and are necessary for the respect of the rights and reputations of others, or for the protection of national security, or public order, or public health or morals.

0.12 As such, after a review of all relevant laws in Malaysia, it is observed that there are a number of laws that are not suitable (and therefore not considered in this Issues Paper) to be used to tackle cyber harassment and the like, as these laws, at its essence, unnecessarily restrict freedom of expression in Malaysia and could create additional barriers to freedom of expression in Malaysia:

- Firstly, criminal defamation set out in section 499 of the Penal Code. The PeopleACT is of the opinion that to couch defamation within the realm of criminal law, which attracts imprisonment and heavy fines, is disproportionate and is not a permissible restriction to freedom of expression. The United Nations Special Rapporteur on Freedom of Expression has continued its call for governments to repeal criminal defamation laws;[6]
- Secondly, the Sedition Act 1948 is unsuitable to be used to tackle the problem of cyberharassment as there is a lack of clarity with regard to fundamentals of the said legislation; this has the potential to leave a negative effect on freedom of expression in Malaysia. In addition, with Malaysia's commitment to the Human Rights Council to address concerns regarding the Sedition Act 1948,[7] the PeopleACT feels that a separate exercise is required to deal with the Sedition Act 1948 to ensure the balance between freedom of expression and restrictions;
- Finally, section 298A of the Penal Code, which makes it an offence for any person who "by words, either spoken or written, or by signs, or by visible representations, or by any act, activity or conduct, or by organizing, promoting or arranging, or assisting in organizing, promoting or arranging, any activity, or otherwise in any other manner (a) causes, or attempts to cause, or is likely to cause disharmony, disunity, or feelings of enmity, hatred or ill will; or (b) prejudices, or attempts to prejudice, or is likely to prejudice, the maintenance of harmony or unity, on grounds of religion, between persons or groups of persons professing the same or different religions". For this provision, the PeopleACT would like to highlight that in the case of *Mamat Daud & Ors v The Government of Malaysia*,[8] the Supreme Court held that section 298A of the Penal Code is invalid and null and void. This was affirmed by the Court of Appeal in the case of *Tan Jye Yee & Anor v PP*.[9]

Issues to be considered

0.13 The People ACT seeks the views of interested parties on the following five issues:

- **Issue 1**: Whether the current provisions in the Communications and Multimedia Act 1998 should be amended to specifically address cyber-harassment and other forms of harmful cyber behaviour;
- **Issue 2**: Whether the current law is sufficient to address online sexual harassment;
- **Issue 3**: Whether current laws prohibiting obscene publications is sufficient to tackle cyberharassment and other harmful cyber behaviour;

[6] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 4 June 2012, A/HRC/20/17, Human Rights Council, Twentieth session, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G12/137/87/PDF/G1213787.pdf?OpenElement> accessed 28 March 2017.

[7] UN Press Release, 'Malaysia Sedition Act threatens freedom of expression by criminalising dissent', 8 October 2014, <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15144#sthash.ZRjfUJs1.dpuf> accessed 28 March 2017.

[8] [1988] 1 CLJ 11.

[9] [2015] 2 CLJ 745.

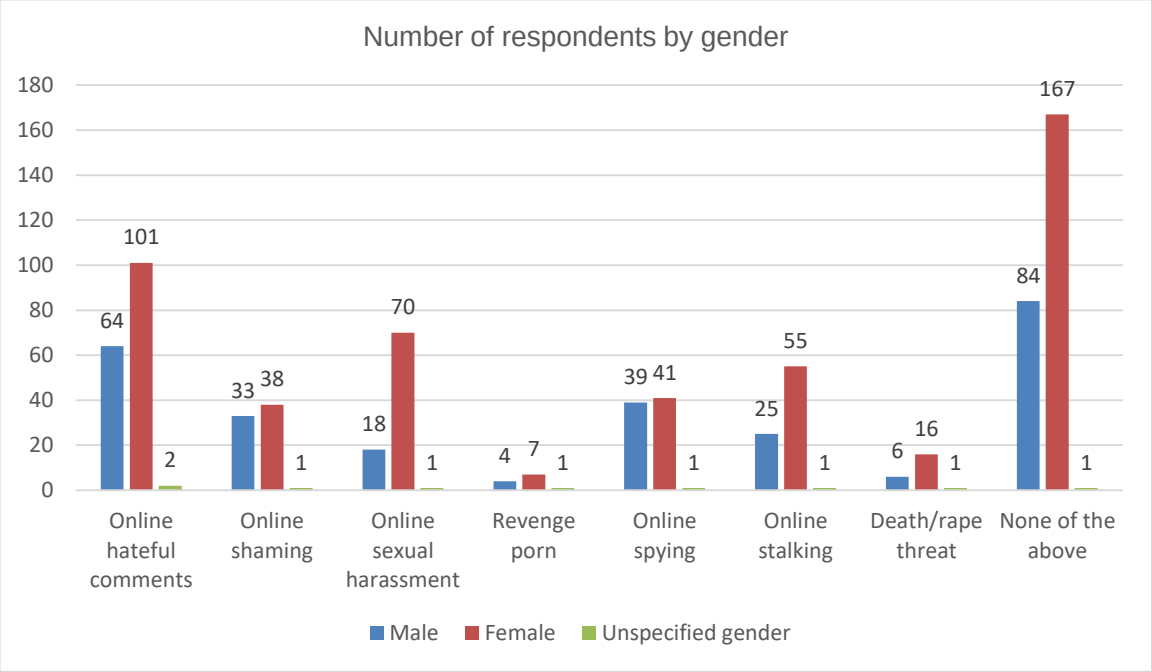
- **Issue 4**: Whether current penal law adequately addresses threats of death and threats of rape and other abusive communications made using cyber technology;
- **Issue 5**: Whether the current law is sufficient to deal with the offence of using cyber technology to seriously interfere with another's privacy.

0.14 Comments may be submitted via email at peopleact@mcchr.org and the PeopleACT will be organising a series of consultation with various groups to obtain their feedback. Thereafter,[10] the PeopleACT will publish a more authoritative report, which will contain the PeopleACT's proposals to the government on the best legal solution to tackling the problem of cyberharassment and other harmful cyber behaviour in Malaysia.

[10] The consultation period will take approximately six months from the date of release of this Issues Paper.

ISSUE 1: WHETHER THE CURRENT PROVISIONS IN THE COMMUNICATIONS AND MULTIMEDIA ACT 1998 SHOULD BE AMENDED TO SPECIFICALLY ADDRESS CYBER-HARASSMENT AND OTHER FORMS OF HARMFUL CYBER BEHAVIOUR

1.1 The problem of cyberharassment and other forms of cyber behaviour is growing in Malaysia as well as globally. In the Survey conducted by the PeopleACT, more than half (50.4percent) of the respondents experienced some form of online harassment, of which 31.6 percent of respondents have been at the receiving end of hateful comments and 17 percent of the respondents stated that they have been sexually harassed.



Number of respondents by gender, who have experienced online harassment

1.2 At this juncture, it is important to point out that across all types of cyberharassment, women experienced more harassment than men and in some categories (online sexual harassment, online death/rape threat, and online stalking), and women were almost twice as likely to have experienced cyberharassment. In addition, women between the age of 17 and 24 years were more exposed to almost all the different types of cyberharassment.

1.3 The above trend corresponds with research carried out globally – according to the Networked Intelligence for Development, 73 percent of women are abused online.[11] Also, women aged between 18 and 24 years face higher risk of being exposed to every kind of cyber violence against women.[12] The prevalence of online harassment and online violence against women occurs because of their gender. This is not a new development – rather the Internet has merely provided another platform for violence, patriarchy, and inequality.

[11] 'Cyber Violence Against Women and Girls – A World-Wide Wake-up Call', A Report by the UN Broadband Commission for Digital Development Working Group on Broadband and Gender, (2015), <http://www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf> accessed 24 March 2016.

[12] 'Cyber Violence Against Women and Girls – A World-Wide Wake-up Call', A Report by the UN Broadband Commission for Digital Development Working Group on Broadband and Gender, (2015), <http://www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf> accessed 24 March 2016.

1.4 Part of the solution to the above is ensuring that the law is able to provide the framework to protect Internet users, with particular attention to online harassment against women.

1.5 Generally, two provisions within the Communications and Multimedia Act 1998 (CMA 1998) are relevant to the subject matter – sections 211 and 233(1) of the CMA 1998.

1.6 Section 211 of the Communications and Multimedia Act 1998 provides that "No content applications service provider, or other person using a content applications service, shall provide content which is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person." Punishment for this offence is a fine not exceeding RM50,000.00 or imprisonment for a term not exceeding one year or to both and a further fine of RM1,000.00 for every day or part of a day during which the offence is continued after conviction.

1.7 Section 233 (1) of the Communications and Multimedia Act 1998 (CMA 1998) creates two offences:

- The first is that it is an offence for a person "(a)…by means of any network facilities or network service or applications service knowingly (i) makes, creates or solicits; and (ii) initiates the transmission of, any comment, request, suggestion or other communication which is obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person;
- The second offence is if a person "(b) initiates a communication using any applications service, whether continuously, repeatedly or otherwise, during which communication may or may not ensue, with or without disclosing his identity and with intent to annoy, abuse, threaten or harass any person at any number or electronic address".

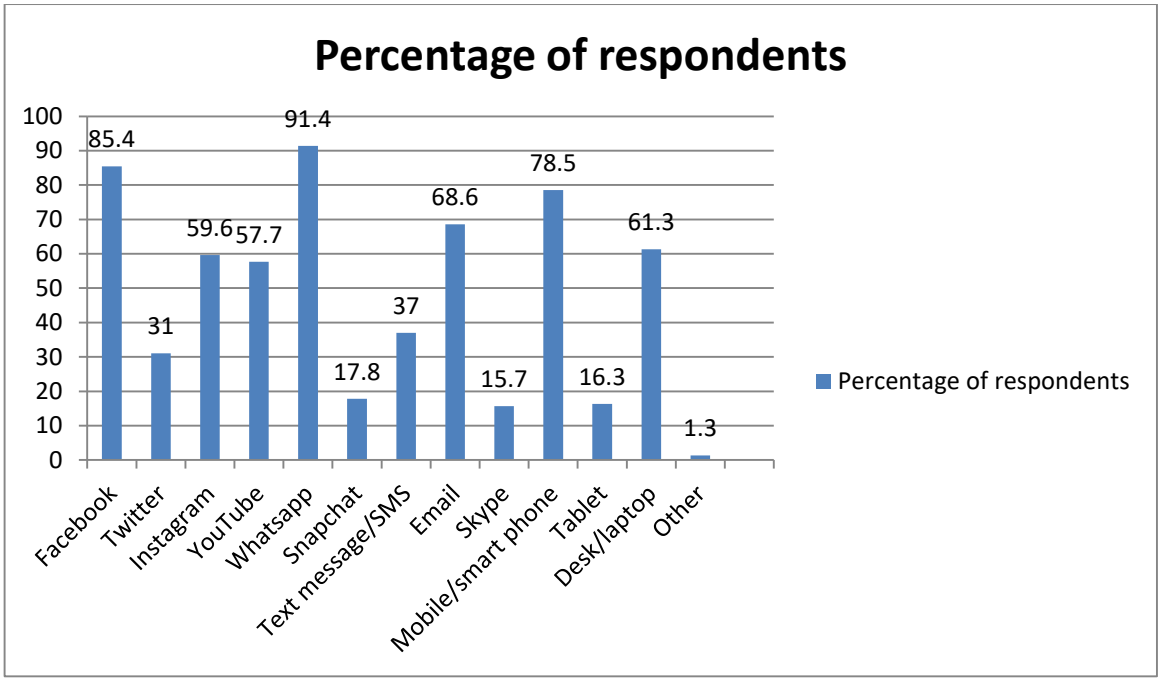
1.8 The punishment for the offence under this section 233(1) is a fine not exceeding RM50,000 or to imprisonment for a term not exceeding one year or to both a further fine of RM1,000 for every day during which the offence is continued after conviction.

Mode/platform and type

1.9 Section 6 of the 1998 Act defines "communications" as "any communication, whether between persons and persons, things and things, or persons and things, in the form of sound, data, text, visual images, signals or any other form or any combination of those forms"; "content applications service" means an applications service which provides content. This includes traditional broadcast services and the latest services such as online publishing and information services;[13] "network facilities" means "any element or combination of elements of physical infrastructure used principally for, or in connection with, the provision of network services, but does not include customer equipment; and "network service" means "a service for carrying communications by means of guided and/or unguided electromagnetic radiation".

1.10 The definition of key words in section 6 means that sections 211 and 233(1) can be applied to cyberharassment as comments and postings (whether written or images) are commonly made using the telephone, email, Facebook, or Instagram. According to the Survey, the top three digital communication platforms used by respondents were WhatsApp (91.4 percent), Facebook (85.4 percent), and email (68.6 percent). As devices, respondents preferred using mobile/smart phones (78.5 percent), desktops (61.3 percent) and tablets (16.3 percent).

[13] Official Portal of The Malaysian Communications And Multimedia Commission <http://www.skmm.gov.my/sectors/celco/licensing.aspx> accessed 21 March 2017.



Types of online, digital communication platform and device used most by respondents on a daily basis

Continuously, repeatedly or otherwise

1.11 It would appear that offences in sections 211 and 233(1) does not require any continuing behaviour on the part of the harasser – this means that a single comment or posting or a barrage of comments or postings (and if other requisite elements are proven) would similarly be caught by either section.

1.12 This is consistent with cases tried under section 233(1) of the CMA 1998, such as *Ahmad Abd Jalil v PP*,[14] *Rutinin v Suhaimin v PP*,[15] and *PP v Chan Hon Keong*,[16] where the accused persons were charged based on one comment made. Only the case of *PP v Muslim Ahmad*[17] involved three offensive comments. In all these cases, the Courts did not deal with the phrase "continuously, repeatedly".

1.13 Section 233(1) (b) is slightly different in that it includes the phrase "continuously, repeatedly…", which could indicate that there is a requirement to show some form of persistence by the harasser. However, the said phrase in section 233(1) (b) also includes the words "… or otherwise", which means that persistence is not an element to be proven.

Communication which is false, menacing or offensive in character

1.14 One common element in sections 211 and 233(1) of the CMA 1998 that must be proven is that the communication or the content must be "obscene, indecent, false, menacing or offensive in character". The words "indecent" and "obscene" will be dealt in greater detail in below in Issue 3; Issue 1 will only look at the words "menacing" and "offensive".

1.15 The CMA 1998 Act does not provide a definition of the words "menacing" or "offensive". Neither has the Courts provided an interpretation of the said words.

[14] [2015] 5 CLJ 480.
[15] [2015] 3 CLJ 838.
[16] [2012] 5 LNS 184.
[17] [2013] 5 CLJ 822.

1.16 From judgements of section 233(1) cases, it is observed that the Courts have held that derisive online comments made against rulers of states amounted to offensive communication. For example, the following comments were found to be offensive - "*Sultan Johor kulitnya putih seperti kulit babi*…";[18] "damn your sultan"; "your sultan *kantoi*"; and "what's the *kantoi* with your sultan";[19] and "Sultan Azlan Kepala Butuh, sia-sia tulis banyak hal perundangan, seolah olah benar-benar Sultan yg *perihatin kepada Rakyat. Cakap lain buat lain ~ dasar hipokrit ! Munafik semua. Lain kali tak payah la undi di Perak, hang pilih la saja siapa siapa yang hang berkenan jadi MB. Ya … tak perlu guna patik atau beta sebab kita bukan hamba raja. Sistem raja hanya satu simbol, tetapi kalau dah dikorup dan dinodai dengan ketidakadilan maka baik dilupuskan saja simbol itu. Biar mati menderhaka, tak enggan hidup diperdaya. akhirnya, hidup mati Tuhan jugak yg menentu*".[20]

1.17 In *PP v Chan Hon Keong*, the Court found the comments offensive because it insulted a reigning Sultan and would reasonably anger and offend the Sultan and any reader or citizen who visits the said webpage. In determining the sentence of the accused person, the Court took into consideration the public interest element stating that members of the public view any insult against the institutional monarchy seriously. Therefore, the offence committed by the accused is a very serious one and if such behaviour (of posting offensive comments against the monarch) is not curbed, it will become a trend.

1.18 Whilst the CMA 1998 and the Courts have not provided any interpretation of what amounts to offensive or menacing communication, Part 1 of the Content Code developed by the Communications and Multimedia Content Forum (CMCF)[21] have provided definitions to key words in sections 211 and 233(1) of the 1998 Act as follows:[22]

- Presentation of violence must avoid the excessive, the gratuitous, the humiliating, and the instructional. The portrayal of violence is permitted to the extent of news reporting, discussion or analysis and in the context of recognised sports events.
- Menacing content – material that causes annoyance, threatens harm or evil, encourages or incites crime, or leads to public disorder. Hate propaganda, which advocates or promotes genocide or hatred against an identifiable group, must not be portrayed. Such material is considered menacing in nature and is not permitted. Information which may be a threat to national security or public health and safety, is also not to be presented.
- Bad language – use of disparaging or abusive words which is calculated to offend an individual or a group of persons is not permitted. Words, in any language commonly used in Malaysia, which are considered obscene or profane are prohibited including crude references to sexual intercourse and sexual organs. It is, however, permissible to use such words in the context of their ordinary meaning and not when intended as crude language.
- Hate speech – this refers to any portrayal (words, speech or pictures, etc.), which denigrates, defames, or otherwise devalues a person or group on the basis of race, ethnicity, religion, nationality, gender, sexual orientation, or disability and is prohibited. In particular, descriptions of any of these groups or their members

[18] *Ahmad Abd Jalil v PP,* [2015] 5 CLJ 480.
[19] *PP v Muslim Ahmad,* [2013] 5 CLJ 822.
[20] *PP v Chan Hon Keong,* [2012] 5 LNS 184.
[21] The CMCF was established pursuant to sections 94 and 212 of the Communications and Multimedia Act 1998. The CMCF is responsible for drafting industry and content codes such as Access Code, Technical Standards Code, Consumer Code, Content Code. The CMCF developed a Content Code and registered it with the MCMC on 1 September 2004. The Code applies to all Content Applications Service Provider, each member of the CMCF, every person who submit their agreement to the CMCF and every person whom the MCMC directed in accordance with section 99 of the Communications and Multimedia Act 1998. However, compliance is on a voluntary basis.
[22] <http://cmcf.my/onlineversion/part2-guidelines-content#1.0> accessed 17 March 2017.

involving the use of strong language, crude language, explicit sexual references or obscene gestures, are considered hate speech.

1.19 Section 1.2 of Part 2 of the Content Code goes further to explain that the standard that contents are measured against is Malaysia's "social, religious, political and educational attitudes and observances" balanced against global diversity. However, it should be noted that the Content Code is not binding

Made with the intent to annoy, abuse, threaten or harass

1.20 The second element in sections 211 and 233(1) of the CMA 1998 is that the impugned communication must be made with the intent to annoy, abuse, threaten, or harass. This was dealt with in passing in *Rutinin v Suhaimin v PP.*[23] In this case, the appellant was accused of posting a comment "Sultan Perak *sudah gilaaaa*". In considering whether the appellant made the comment with intent to abuse or harass, the High Court (in an appeal) overturned the conviction of the appellant on the grounds that the prosecution did not adduce evidence that it was the appellant who actually made and initiated the transmission of the impugned comment – the prosecution merely inferred that since the computer and the Internet account belonged to him that he made the said comment. This inference tantamount to invoking a presumption against the appellant which the law did not allow.

1.21 Section 233(1) of the CMA 1998 does not explicitly mention whether the test is an objective or subjective one.

Indirect cyberharassment

1.22 Indirect cyberharassment is "persistent harmful online communications to third parties concerning a complainant but not directly communicated to the complainant".[24] An example of indirect online harassment is when a person posts harmful comments on a social media platform not directly to the victim/survivor but to social media sites maintained by the victim/survivor's friends and family members; or when a person makes harmful comments to the public about the victim/survivor.[25]

1.23 Section 233(1)(b) of the CMA 1998 appears to cover the offence of indirect cyber harassment as the offence is to initiate a communication with the intent to annoy, abuse, threaten or harass ***any person*** (emphasis added). This implies that the impugned communication need not be directed at the victim/survivor and could encompass the situations mentioned above.

Other jurisdictions

United Kingdom

1.24 In the UK, although there are no specific laws to deal with cyberharassment and other harmful cyber behaviour, there are a number of laws that explicitly provides for the offences of harassment,[26] putting people in fear of violence,[27] stalking, stalking involving

[2323] [2015] 3 CLJ 838.

[24] Law Reform Commission, 'Issues Paper on Cyber-crime affecting person safety, privacy and reputation including cyber-bullying (LRC IP 6-2014), <http://www.lawreform.ie/_fileupload/Issues%20Papers/ip6Cybercrime.pdf> accessed 20 April 2016.

[25] Law Reform Commission, 'Issues Paper on Cyber-crime affecting person safety, privacy and reputation including cyber-bullying (LRC IP 6-2014), <http://www.lawreform.ie/_fileupload/Issues%20Papers/ip6Cybercrime.pdf> accessed 20 April 2016.

[26] Section 1(1) of the Protection From Harassment Act 1997 states that "a person must not pursue a course of conduct – (a) which amounts to harassment of another, and (b) which he knows or ought to know amounts to harassment of the other".

[27] Section 4(1) of the Protection From Harassment Act 1997 states that when a "person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him, is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions".

fear of violence or serious alarm or distress, and sending malicious or grossly offensive communications.

1.25 The first four offences mentioned above (harassment, putting people in fear of violence, stalking, stalking involving fear of violence or serious alarm or distress) can be found in the Protection from Harassment Act 1997. The definitions of these offences are as follows:

- **Harassment.** Section 7 of the 1997 Act states that "harassing a person" includes "alarming the person or causing the person distress". The UK Crown Prosecution Service (CPS) 'Stalking and Harassment Legal Guidance' explains that harassment could include "repeated attempts to impose unwanted communications and contact upon a victim in a manner that could be expected to cause distress or fear in any reasonable person".[28] Examples of cases include *Plavelil v Director of Public Prosecutions,*[29] where the Court held that repeated faxes of false and malicious assertions amounted to a course of harassment; in *R v Debnath*,[30] the Court held that appellant's conduct of sending to the complainant's fiancée, emails purporting to be from one of his friends, informing her of alleged sexual indiscretion; registering the complainant on a website called "positivesingles.com", a database for people with sexually transmitted disease; and setting up a website called "A is gay.com", which had a fake newspaper article detailing alleged homosexual practices by the complainant, which resulted in the complainant received large amounts of homosexual pornography, amounted to harassment.

- **Stalking.** As for the offence of stalking, section 2A(3) of the Protection from Harassment Act 1997 lists out a number of examples of behaviours associated with stalking as follows:
  - following a person,
  - contacting, or attempting to contact, a person by any means,
  - publishing any statement or other material - (i) relating or purporting to relate to a person, or (ii) purporting to originate from a person,
  - monitoring the use by a person of the internet, email or any other form of electronic communication,
  - loitering in any place (whether public or private),
  - interfering with any property in the possession of a person,
  - watching or spying on a person.
- According to the CPS, section 2A(3) is not an exhaustive list and it will be open to the courts to consider other acts by a defendant and conclude whether those acts constitute stalking even if they are not listed in section 2A(3). Additionally, the CPS clarified that harassment that includes any one or more of the above behaviour is not automatically stalking – the course of conduct, assessed as a whole, must fit the generally received interpretation of the word stalking.[31]

- **Stalking involving fear of violence or serious alarm or distress**. Section 4A of the 1997 Act creates an offence of stalking involving fear of violence or serious alarm or distress. The elements of this offence include, a person whose course of conduct amounts to stalking, and either (i) causes another ("B") to fear, on at least two occasions, that violence will be used against B, or (ii) causes B serious alarm or distress which has a substantial adverse effect on B's usual day-to-day activities.

[28] <http://www.cps.gov.uk/legal/s_to_u/stalking_and_harassment/> accessed 9 January 2017.
[29] [2014] EWHC 736 (Admin).
[30] [2005] EWCA Crim 3472.
[31] <http://www.cps.gov.uk/legal/s_to_u/stalking_and_harassment/> accessed 9 January 2017.

- The phrase “substantial adverse effect on B's usual day-to-day activities” is not defined but the guidelines issued by the Home Office suggests that evidence of a substantial adverse effect may include:[32]
  - the victim changing their routes to work, work patterns, or employment;
  - the victim arranging for friends or family to pick up children from school (to avoid contact with the stalker);
  - the victim putting in place additional security measures in their home;
  - the victim moving home;
  - physical or mental ill-health;
  - the deterioration in the victim's performance at work due to stress;
  - the victim stopping /or changing the way they socialise.
- Section 4A does not require any particular stalking incident to be alarming or serious; rather the cumulative effect of the stalking is important.[33]

- **Cyber stalking**. Whilst the 1997 Act does not provide for the offence of cyber stalking, the CPS acknowledged that stalking can take place on the Internet and has provided examples of the use of the Internet, social networking sites, chat rooms, emails or other forums facilitated by technology:[34]
  - to locate personal information about the victim;
  - to communicate with the victim;
  - as a means of surveillance of the victim;
  - identity theft such as subscribing the victim to services, purchasing goods and services in their name;
  - damaging the reputation of the victim;
  - electronic sabotage such as spamming and sending viruses; or
  - tricking other Internet users into harassing or threatening a victim.
- The CPS Social Media Guidelines for Prosecutors provides the following examples of cyber-stalking:[35]
  - Threatening or obscene emails or text messages;
  - Spamming, where the offender sends the victim multiple junk emails;
  - Live chat harassment or 'flaming', a form of online verbal abuse;
  - "Baiting", or humiliating peers online by labelling them as sexually promiscuous;
  - Leaving improper messages on online forums or message boards;
  - Unwanted indirect contact with a person that may be threatening or menacing, such as posting images of that person's children or workplace on a social media site, without any reference to the person's name or account;
  - Posting "photoshopped" images of persons on social media platforms;
  - Hacking into social media accounts and then monitoring and controlling the accounts;
  - Sending electronic viruses;
  - Sending unsolicited email;
  - Cyber identity theft.

1.26 For all of the above offences, there must be evidence to prove the conduct was targeted at an individual, was calculated to alarm or cause him/her distress, and was oppressive and unreasonable.[36] Additionally, the prosecution must prove that the conduct is unacceptable to a degree which would sustain criminal liability.

---

[32] <http://www.cps.gov.uk/legal/s_to_u/stalking_and_harassment/> accessed 9 January 2017; see also <https://www.gov.uk/government/publications/a-change-to-the-protection-from-harassment-act-1997-introduction-of-two-new-specific-offences-of-stalking> accessed 10 January 2017.
[33] <http://www.cps.gov.uk/legal/s_to_u/stalking_and_harassment/> accessed 9 January 2017.
[34] <http://www.cps.gov.uk/legal/s_to_u/stalking_and_harassment/> accessed 9 January 2017.
[35] <http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/#a08> accessed 2 February 2017.
[36] <http://www.cps.gov.uk/legal/s_to_u/stalking_and_harassment/> accessed 9 January 2017.

1.27 What is rather interesting with regard to the aforementioned offences is that to prove these offences, the harasser must pursue "***a course of conduct*** which amounts to harassment of another" (emphasis added). Section 7 of the Protection of Harassment Act 1997 defines "course of conduct" to mean "at least two occasions and in relation to a single person". As regards the time period between occasions, the 1997 Act does not specify this but according to the CPS, so long as the behaviour complaints of ceased, even for a short period of time, and then resumed, either in the same or different form, this can form a course of conduct. However, if there are only two incidents and a long period between them, the less likely it is that the courts will accept it as amounting to a course of conduct. Each case will be determined on its own facts. For example, in the case of *Pratt v DPP,*[37] the Administrative Court held that two incidents almost three months apart were "close to the line" but nevertheless sufficient to establish a course of conduct within the meaning of the 1997 Act.[38]

1.28 The 1997 Act expressly states that the test to be applied to prove harassment or putting people in fear of violence or stalking is an objective one, i.e. that the person whose course of conduct is in question ought to know that it amounts to, harassment or putting people in fear of violence or stalking of another, if a reasonable person in possession of the same information would think the course of conduct amounted to harassment of the other.[39]

1.29 Apart from the Protection from Harassment Act 1997, the UK Communications Act 2003, specifically sections 127(1) and (2) have been used to tackle cyber harassment and other harmful cyber behaviour. The 2003 Act is somewhat similar to the Malaysian CMA 1998 - sections 127(1) and (2) creates two offences of sending by means of a public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or causes any such message or matter to be so sent (section 127(1)); and sending by means of a public electronic communications network, a message that he knows to be false; causes such a message to be sent; or persistently makes use of a public electronic communications network (section 127(2)). Sections 127(1) and (2) applies to messages sent by Twitter as it is considered a message sent via "public electronic communications network".[40]

1.30 According to the CPS, Section 127(2) targets false messages and persistent misuse intended to cause annoyance, inconvenience or needless anxiety; it includes somebody who persistently makes silent phone calls.[41]

1.31 Mindful of the need to respect freedom of expression and that sections 127(1) and (2) are not used to unnecessarily curb freedom of expression, the CPS reminded prosecutors that regard should be had to the context in which interactive social media dialogue takes place as opposed to other communications. Banter, jokes and offensive comments are commonplace and often spontaneous and communications intended for a few may reach millions.[42] As such, prosecutors should only proceed with cases under section 1 of the Malicious Communications Act 1988 and section 127 of the Communications Act 2003 where they are satisfied there is sufficient evidence that the communication in question is ***more than*** (emphasis added)***:***

- Offensive, shocking or disturbing; or

[37] [2001] EWHC 483.
[38] <http://www.cps.gov.uk/legal/s_to_u/stalking_and_harassment/> accessed 9 January 2017.
[39] See sections 1(2), 4(2), 4A of the Protection of Harassment Act 1997.
[40] *Chambers v DPP*, [2012] EWHC 2157 (Admin).
[41] http://www.cps.gov.uk/legal/a_to_c/communications_offences/
[42] Guidelines on prosecuting cases involving communications sent via social media, The Crown Prosecution Service (UK), <http://www.legislation.gov.uk/ukpga/2015/9/section/76> accessed 6 February 2017.

- Satirical, iconoclastic or rude comment; or
- The expression of unpopular or unfashionable opinion about serious or trivial matters, or banter or humour, even if distasteful to some or painful to those subjected to it.

1.32 The Courts have interpreted “menacing character” to mean a communication that creates fear and apprehension in those whom it is communicated, or may reasonably be expected to see it.[43] As to what amounts to “grossly offensive”, the test was established in *DPP v Collins*.[44] In this case, the respondent made a number of phone calls to the Westminster offices of Mr David Taylor, the Member of Parliament for North West Leicestershire. Some of the messages he left included reference to "Wogs", "Pakis", "Black bastards" and "Niggers". The House of Lords held that "grossly offensive" requires more than simply offensive; just because the communication is in bad taste, controversial or unpopular and may cause offence to individuals or a specific community, this is not in itself sufficient reason to engage criminal law. Lord Bingham stated that:
- “There can be no yardstick of gross offensiveness otherwise than by the application of reasonably enlightened, but not perfectionist, contemporary standards to the particular message sent in its particular context. The test is whether a message is couched in terms liable to cause gross offence to those to whom it relates. The Justices must apply the standards of an open and just multi-racial society;
- The question is whether the defendant used language which is beyond the pale of what is tolerable in our society;
- Is there anything in the content or tenor of the messages to soften or mitigate the effect of the language in any way?”

1.33 The case of *DPP v Collins* was interesting in that the Courts held that it did not matter that the message that caused gross offence were not the recipients.

1.34 Another relevant legislation in the UK is the Malicious Communications Act 1988 where section 1(1) makes it an offence for a person to send to another person a letter or other article which conveys (i) a message which is grossly offensive. The sender must intend to cause distress or anxiety to the recipient or to any other person to whom he intends that it or its contents or nature should be communicated. The punishment (upon summary conviction) for the aforementioned offence is a fine not exceeding level 4 on the standard scale (section 1(4)).

1.35 According to the CPS, section 1 of the Malicious Communications Act 1988 “covers letters, writing of all descriptions, electronic communications, photographs and other images in a material form, tape recordings, films and video recordings. The offence is one of sending, delivering or transmitting, so there is no requirement for the article to reach the intended recipient”.[45]

1.36 In the case of *Connolly v DPP* [2007] 2 All ER 1012, the phrase "indecent or grossly offensive" in section 1 were said to be ordinary English words. The fact that there was a political or educational motive behind the accused sending graphic photographs of aborted foetuses did not help her, and her argument that her behaviour was protected by Articles 9 and 10 ECHR (freedom of religion and speech) did not succeed, because the restrictions on those rights were justified under Articles 9(2) and 10(2).

Ireland

[43] *Chambers v DPP*, [2012] EWH2 2157 (Admin).
[44] [2006] 1 WLR 2223.
[45] <http://www.cps.gov.uk/legal/a_to_c/communications_offences/> accessed 6 February 2017.

1.37 Ireland recently passed a specific law to deal with cyberharassment. The Harmful and Malicious Electronic Communications Act 2015, creates two offences with regard to electronic communications:[46]

- **Offence of harmful electronic communication**. Section 3 of the Harmful and Malicious Electronic Communications Act 2015 makes it an offence for any person who without lawful authority or reasonable excuse, intentionally or recklessly shares a harmful electronic communication. "Harmful electronic communications" is defined as one that:
  "(a) incites or encourages another to commit suicide,
  (b) incites or encourages another to cause serious harm to themselves, or
  (c) includes explicit content of the other,
  and it intentionally or recklessly causes alarm, distress or harm to the other."

- **Offence of malicious electronic communication**. Section 4 of the 2015 Act makes it an offence for a person who, "without lawful excuse, persistently shares malicious electronic communications regarding another…an electronic communication shall be considered malicious where it intentionally or recklessly causes alarm, distress or harm to the other".

1.38 For the purposes of the two sections above, "shares" is defined in section 2 of the 2015 Act to include "sending, posting, distributing or publishing on the internet an electronic communication". For both offences, the penalty for those found guilty is a fine not exceeding EUR5,000 or imprisonment for a term not exceeding 12 months or both.

1.39 As the law has just been passed, there are no reported cases.

1.40 Prior to the 2015 Act, the Non-Fatal Offences Against the Person Act 1997 was used to deal with cases of cyber harassment. Section 10(1) of the Non-Fatal Offences Against the Person Act 1997 states that a person "(1)…who, without lawful authority or reasonable excuse, by any means including by use of the telephone, harasses another by ***persistently*** (emphasis added) following, watching, pestering, besetting or communicating with him or her, shall be guilty of an offence. (2) For the purposes of this section a person harasses another where— (a) he or she, by his or her acts intentionally or recklessly, seriously interferes with the other's peace and privacy or causes alarm, distress or harm to the other, and (b) his or her acts are such that a reasonable person would realise that the acts would seriously interfere with the other's peace and privacy or cause alarm, distress or harm to the other."

1.41 The punishment for the section 10 offence is imprisonment not exceeding 12 months (on summary conviction) or seven years imprisonment (on indictment conviction). The court may also issue a restraining order to restrain the defendant from communicating with the claimant, restraining order, or a restriction on movement order

1.42 Similar to the UK Protection from Harassment Act 1997, section 10 of the Irish Non-Fatal Offences Against the Person Act 1997 requires persistent conduct for the offence of harassment. "Persistently" was interpreted in *Director of Public Prosecutions (O'Dowd) v Lynch*[47] to mean "behaviour that is continuous and can include either a) a number of

[46] Section 3 of the Harmful and Malicious Electronic Communications Act 2015 makes it an offence for any person who without lawful authority or reasonable excuse, intentionally or recklessly shares a harmful electronic communication. Section 4 of the 2015 Act makes it an offence for a person who, "without lawful excuse, persistently shares malicious electronic communications regarding another".

[47] [2008] IEHC 183, unreported, High Court, 5 June 2008. In this case the accused had been charged in the District Court with an offence of harassment contrary to section 10 of the Act. He had admitted that he had indecently exposed himself to two children at their home on four separate occasions during the course of an afternoon. The High Court held that it was satisfied that the requirement of persistence

incidents that are separated by intervening lapses of time, or b) a single but continuous incident such as following a person on an unbroken journey over a prolonged distance".[48]

1.43 Examples of successful cases prosecuted under section 10 of the Non-Fatal Offences Against the Person Act 1997 include a man who sent 500 offensive text messages to a teenage boy, calling the teen "gay boy", "f***ing bitch" and warned that a group of people would "teach you a lesson";[49] and a man who, over a period of eight months, posted vile sexual messages about his ex-girlfriend on a website, "messages suggesting that she was inviting men to get in touch with her for sex" and her name and address.[50]

Australia

1.44 In Australia, there are specific provisions in the Criminal Code Act 1995 that deal with cyberharassment and other harmful cyber behaviour:

- Using a carriage of service to threaten to kill and another person (section 474.15);
- Using a carriage of service to threaten to cause serious harm; this includes a threat to substantially contribute to serious harm to the person (section 474.15);
- Using a carriage service directly or indirectly counsels or incites that person to commit or attempt to commit suicide (section 474.29A);
- Using a carriage service; and the person does so in a way (whether by the method of use or the content of a communication, or both) that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive" (section 474.17);
- Distributing an invasive image of another person, "knowing or having reason to believe that the other person: (a) does not consent to that particular distribution of the image; or (b) does not consent to that particular distribution of the image and does not consent to distribution of the image generally".[51] "Invasive image" means a moving or still image of a person engaged in a "private act", or in a state of undress "such that the person's bare genital or anal region is visible"; and "private act" means a "sexual act of a kind not ordinarily done in public, an act carried out in a sexual manner or context or using the toilet" (section 26C(1) of the Summary Offences Act 1953 of South Australia);
- Stalking - on at least two separate occasions…(iv) gives or sends offensive material to the other person, or leaves offensive material where it will be found by, given to or brought to the attention of the other person; or (iva) publishes or transmits offensive material by means of the internet or some other form of electronic communication in such a way that the offensive material will be found by, or brought to the attention of, the other person; or (ivb) communicates with the other person, or to others about the

was fulfilled by incidents which were separated by intervening lapses of time as in the present case and secondly incidents capable of being severed even if they are not so severed or immediately succeed each other, Annual Report 2008, Office of the Director of Public Prosecutions, <https://www.dppireland.ie/filestore/documents/Annual_Report_2008_ENG.pdf> accessed 10 October 2016.

[48] Law Reform Commission, 'Issues Paper on Cyber-crime affecting person safety, privacy and reputation including cyber-bullying (LRC IP 6-2014), <http://www.lawreform.ie/_fileupload/Issues%20Papers/ip6Cybercrime.pdf> accessed 20 April 2016.

[49] Law Reform Commission, 'Issues Paper on Cyber-crime affecting person safety, privacy and reputation including cyber-bullying (LRC IP 6-2014), <http://www.lawreform.ie/_fileupload/Issues%20Papers/ip6Cybercrime.pdf> accessed 20 April 2016.

[50] John Fallon, 'Man avoids jail for 'vile' internet messages about ex-girlfriend', 20 March 2014, *Irish Times*, <http://www.irishtimes.com/news/crime-and-law/courts/man-avoids-jail-for-vile-internet-messages-about-ex-girlfriend-1.1731368> accessed 20 July 2016.

[51] It is a defence to a charge of an offence against this section to prove - (a) that the conduct constituting the offence - (i) was for a purpose connected to law enforcement; or (ii) was for a medical, legal or scientific purpose; or (b) that the image was filmed by a licensed investigation agent within the meaning of the Security and Investigation Agents Act 1995 and occurred in the course of obtaining evidence in connection with a claim for compensation, damages, a payment under a contract or some other benefit and the distribution of the image was for a purpose connected with that claim.

other person, by way of mail, telephone (including associated technology), facsimile transmission or the internet or some other form of electronic communication in a manner that could reasonably be expected to arouse apprehension or fear in the other person…and the person (i) intends to cause serious physical or mental harm to the other person or a third person; or (ii) intends to cause serious apprehension or fear (section 19AA of the Criminal Law Consolidation Act 1935 of South Australia).

1.45 Unlike UK and Irish law, save for the offence of stalking, the Australian Criminal Code Act 1995 does not explicitly require persistent behaviour as an element of the offence. However, the cases prosecuted under section 474.17 appear to show that persistent behaviour from the harasser is a contributing factor in finding guilt. In *R v Ogawa*,[52] the appellant sent 83 emails during an 18 hour period, made 176 phone calls to the Federal Court registries and chambers. The communications included threats to a barrister and associate to the chief justice, to kill two Federal Court registrars with whom she had previously dealt with. Charged under section 474.17 of the Criminal Code Act 1995,[53] the Court sentenced her to six months imprisonment on each charge to be served concurrently.

1.46 Also, section 474.17 of the Criminal Code Act 1995 explicitly states that the test is an objective one where a reasonable person would regard it as menacing, harassing or offensive.

1.47 Persistent behaviour is required to be proven in stalking offences where section 19AA states that the offence of stalking comprises "at least two separate occasions". The first case for cyber stalking was in the much publicised case of Shane Gerada; Gerada sent over 300 threatening text messages to 17-year-old Allem Halkic over the course of a few months. Over two days in February, Gerada sent Halkic five particularly aggressive messages, one that read, "Ur all mouth and no action, wait till I get my hands on u, and I'm telling u now ill put you in hospital."[1] Gerada also used the MySpace social-networking site to falsely claim that Halkic had formed a relationship with another friend's girlfriend.[2] Soon after these events Halkic committed suicide.[54] Shane Phillip Gerada, 21, pleaded guilty in the Melbourne Magistrates Court to stalking.[55]

1.48 In *Phillips v Police*,[56] the appellant and MH were acquainted through their involvement in training of young cyclists. MH heard rumours that the appellant had acted inappropriately toward young women and MH passed on the information and as a result the appellant was suspended from the training. MH became a police officer in 2009. In court, MH testified that in 2013, he received a series of private Facebook messages from the appellant alleging that MH had unlawful sexual relationships with B and another young female cyclist, C. The appellant threatened to inform the police about MH's relationship with the young women and warned that MH would probably be imprisoned for his conduct. MH sent private Facebook messages to the appellant asking him to stop, threatening defamation proceedings. The appellant stopped sending him private Facebook messages. MH then blocked the appellant as a Facebook friend. In January 2014 MH was shown a screenshot of a public Facebook post made by the appellant:

[52] [2009] QCA 307.
[53] Section 474.17 of the Criminal Code Act 1995 states that a person commits an offence if "the person uses a carriage service; and the person does so in a way (whether by the method of use or the content of a communication, or both) that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive".
[54] 'Cyberbullying in Australia (3 May 2013), <https://cybercrime2013.wordpress.com/2013/05/03/australian-cases/> accessed 8 November 2016.
[55] 'Cyber bully whose victim suicided avoids jail', *The Daily Telegraph*, 8 April 2010, <http://www.dailytelegraph.com.au/cyber-bully-whose-victim-suicided-avoids-jail/story-e6freuz0-1225851552210> accessed 8 November 2016.
[56] [2016] SASC 135 (19 August 2016).

- "THE BITCH WHO STABBED ME, is back in JAIL, locked up yesterday afternoon, clever little bitch is she!!! Oh well [MH] shes locked up again so its back to [B] or that other young thing youve been training with, you know, the one who rides in your top which is sizes too big for her....OH, why here, you blocked me fag. TRUTH HURTS mutha fuka!! COPS dont lie....Youll get to the big house yet you prick!!!-[emo] feeling excited.
- [MH] the corrupt cop, is finally being investigated for accessing my police files when not authorised to do so, three times to get my phone numbers and call and harass and threaten me. About time, this corrupt bastard should not be a cop, broken a guys arm while he was in his police custody too, the dirty bastard. He was the one fucking the bitch who stabbed me when she was 15/16, HE WAS HER COACH, they pinned it all on me the sons of bitches, KARMA IS A BITCH ISNT IT [MH], time for the big house mutha fucker, time to be butt fucked [MH], you would luv it hey, its your favourite I'm told!!!! Oh you blocked me mate after threatening me with private messages!!!! Here it is big boy, you fucking hero. LIKE IT NOW, I might pass on the rest of the info I have, you cant get her to come and stab me again, she is in prison, gonna make [B] do it, the other one you fucked when she was 16..... SUFFA BITCH!!!"

1.49 The Magistrates Court held that the accusations (taken separately or together) are of such a nature that they are calculated to wound the feelings or arouse anger, resentment, disgust or outrage in the mind of a reasonable person. Also, such accusations, did arouse in MH and have the capacity to cause a reasonable person to become apprehensive or fearful for their reputation, apprehensive or fearful that they might be embarrassed in front of their partner family and friends apprehensive or fearful that they might be embarrassed in front of their colleagues and associates, apprehensive or fearful that they might be embarrassed in front of their employer. What is significant in this case is that the Magistrates Court held that section 19AA(1)(b) of the Criminal Law Consolidation Act 1935 of South Australia does not stipulate that an offender must intend to bring about the physical or mental harm in a particular way. Nor does the section expressly require that the apprehension or fear, which an offender intends to cause, must be of physical harm or death; and the definition of stalking in section 19AA(1) extends to an apprehension or fear of any adverse consequence which is accompanied by anxiety or emotional distress which interferes with a person's social, family or working life.

Analysis

Specific offences

1.50 A perusal of the relevant laws in the UK, Ireland and Australia measured against the CMA 1998 show that legislation in these jurisdictions deals with cyberharassment and other harmful cyber behaviour in a more comprehensive way. Firstly, the legislation contains specific offences that spell out the many types of cyberharassment, such as harassment, stalking, death threats, communication that incites or encourages another to commit suicide or to harm themselves, and communication that includes explicit content of another person. In addition, the respective laws define the elements of the offence of harassment or stalking and in particular in the UK, the CPS issues guidance on these laws, which sets out examples of behaviour that could amount to stalking or harassment. The CPS guidance is instructive as it provides a benchmark upon which members of the public are able to use to guide their conduct online.

1.51 Also, it is pertinent to note that the UK Communications Act 2003 which is similar to the CMA 1998 proscribes ***grossly*** offensive communication (emphasis added) and not mere offensive communication. This sets a higher threshold and according to the CPS, prosecutors must only proffer a charge if the communication is ***more than*** (emphasis added) offensive, shocking or disturbing; satirical, rude, unpopular, unfashionable,

painful or distasteful comments do not fall within the definition of grossly offensive communication.

1.52 In Ireland, it is interesting that apart from causing alarm, distress or harm, the definition of harassment could also mean interference into the other person's peace and privacy. This essentially brings into the concept of harassment an individual's right to privacy.

1.53 In contrast, section 233(1) of the CMA 1998 contains a rather general offence of making an obscene, indecent, false, menacing or offensive comment with the intention to annoy, abuse, threaten or harass another person.

1.54 Offensive communication online is nothing new in Malaysia. According to the Survey report, 77 percent of respondents considered hateful comments as online violence.[57]

1.55 The Survey also showed that 31.9 percent of respondents received hateful comments online. This was the highest type of online harassment experienced by respondents, by both men and women alike, and in all age groups. Similarly, a survey carried out by the PeopleACT with the lesbian, gay, bisexual, transgender, intersex or queer (LGBTQI) community, showed that the LGBTQI community were equally susceptible to online hateful comments (28.4 percent) and online stalking (26.9 percent).

1.56 Some of the offensive remarks from incident reports include:

> *"If you were my patient, I'll inject you with poison."*

> *"Ambik dia berlakon dalam tanah kubur….bagi dia rasa sikit macamana keadaan orang macam dia bila tiba hari kematian…kot kot dia insaf;" "Babi punya babi gemuk ni…dah boleh jatuh munafik dasar babi gemuk ni;" "Cibai anak babi la ko ni…apalah nasib mak bapak yang melahirkan ko ni…..mesti dia kecewa lahirkan anak babi macam ni….semua ni usaha-usaha memesongkan akal orang Islam la ni sebab-sebab dia buat kenyataan macam ni…kimak punya kafir sesat…tembak je bagi mampos..haram jadah…muka dahlah macam syaitan….puiii;" "Bila la dia nak mati?;" "If it were up to me, I would have chopped off this [name of the survivor] head already...traitor to the religion and destroyer of the faith of Muslims in these times".*

> *Aku penggal kepala kau. Kepala anak sulung kau aku belah. Kau sundal. Anak kedua kau babi" and "Aku lapah kau. Jantung kau aku rentap*

> *Doctored image of Bersih chief [name of survivor A] and A's three sons, [name of survivor B], and [name of survivor C] kneeling in front of a man holding a large knife clad in a balaclava were sent twice to A's phone between October and November 2016. The image was accompanied by the message, "In the name of Allah, and the sanctity of the Islamic struggle in Malaysia, if you want to lose your head like in Syria, continue with your stupid work. I will ¬decapitate you, record it and spread it on You Tube. I know who you are, I know where you live and I know your family and children. This warning is from Islamic State Malaysia."*

[57] In this context, respondents were asked whether the following would be considered online violence - "When someone demeans you by calling you names or insults targeted at your gender, race, religion, political views, e.g. kafir habir, deviant, whore.."

In 2013, a survivor shared a picture of his/her premature son on Instagram and that attracted at least ten offensive comments, such as, "I will go to the hospital where fighter [a nickname given to the baby by the parents] is and I will apply euthanasia right away #notoanimalcuelty"; "Fighter seems to look like an #alien but he is a real baby so let's just pray for his health and anyway his face can be fixed by #camera360;" "Don't worry, we will support you financially but let us sell his organ to make money out of it! And we will just help to cremate him after. He doesn't deserve to suffer to be old like you;" "Advance #condolence and we will miss you FIGHTER."

"Kepala hotak kau…kalau aku jumpa kau….aku bunuh terus. Buat malu orang Islam je, Kau ni aku layak perangi atas jihad demi menegakkan agama Islam. Aku perangi kau! Aku perangi kau!! Takbir;" "Hahahaha….I wish I could behead you. Typical, non-Muslim;" "Dengan nama Allah, kerajaan bagi greenlight bunuh, akulah orang pertama akan offer bunuh dia ni;" "Kasi bunuh ini perempuan, memalukan kaum, bangsa dan agama. Sesat;" "DARAH ORANG YANG MENGHINA ISLAM NI, HALAL UNTUK DIBUNUH!" "Orang yang hina Islam macam ni sepatutnya kena tembak je bagi mampus"; "Best example of a lonely attention seeking bitch!!! A swab test on her mouth would probably prove that she blows these dogs…haha."

"Aku on the way ke rumah [name of survivor]. Aku akan masuk ikut bilik. Once aku dah atas katil, mohon siapa-siapa roger Pegawai Penyiasat Agama (PPA). Kalau kesiankan aku, roger esok malamlah. At least, aku boleh try dia dulu malam ini ," This was posted with a "feeling wonderful" Facebook emotion.

1.57 Whilst these comments may or may not amount to grossly offensive communication, the data collected illustrates that hateful and contemptuous comments are unfortunately commonplace. And the longer a person spends his or her time online, the more he or she experiences hateful comments.

	Percentage (%) of respondents who spent:		
No. of hours spent online/per day / **Experience**	**0 – 5 hours/day**	**6 – 10 hours/day**	**More than 10 hours/day**
Hateful comment	28%	40%	57%
Online shaming	12%	25%	36%
Revenge porn	1.4%	7.5%	14%
Death/rape threat	3%	5%	7%

Experience of online violence measured against the length of time spent online per day

Key words are expressly defined

1.58 Secondly, the laws and/or case law in the UK, Ireland and Australia define key words in the relevant legislation. For example, the UK courts have interpreted the phrase "menacing character" and have established a comprehensive test of "grossly offensive" and the standard to be applied is an open and just multi-racial society. Also, the newly passed Irish Harmful and Malicious Electronic Communications Act 2015 clarifies with specificity "harmful electronic communications" to include only three instances – inciting or encouraging another to commit suicide or harm themselves, or communication that includes explicit content of the other person.

Persistence is required

1.59 Thirdly, most of the anti-cyberharassment laws require that the harassing or stalking behaviour to be persistent. Section 7 of the UK Protection of Harassment Act 1997, section 19AA of the Criminal Law Consolidation Act 1935 of South Australia, and section

10(1) of the Non-Fatal Offences Against the Person Act 1997, all require more than one incident to be committed against the victim/survivor. The law in UK and Australian require at least two occasions and the Irish law does not prescribe any minimum number of incidents – the law merely states "persistently".

1.60 Incidents collated by the PeopleACT show that hurtful comments (with some receiving more than 100 such comments/message) sent to victims/survivors are unrelenting and likely to meet the persistence/ course of conduct threshold:

> *In May 2015, a survivor posted a photo of a man hitting a woman's head on a plane. Subsequently, he/she received about 100 private messages a day on Facebook. Most of them criticised his/her interference and were accompanied by racist comments and threats such as "cina babi" (Chinese pig), "I tolong you balik Cina" (I help you to return to China), and "don't let me see you." He/she continued to receive hurtful and hostile comments online for two months and admitted to fearing for his/her life. During that period, he/she hid at home and deactivated his/her Facebook account temporarily.*

> *In 2016, a survivor posted his/her experience of being harassed at a restaurant for eating during Ramadhan on Facebook. Allegedly, the said post was translated to Malay by two prominent bloggers; the post became viral and was shared close to 10,000 times on Facebook. Subsequently, the survivor received many hateful comments, such as: -"Bodoh macam lembu; ""Kamu harus menulis dalam Bahasa Melayu biar semua orang Melayu Islam faham bahawa kamu ni amat memalukan. Shame on you.;" "So perempuan macam ni sekarang kalau period, memang tak kisah nak bagi tau semua orang yang kau period?? Baik pakai tag besar tulis, I'm period, and I am free to eat in public in Ramadhan." The survivor's family was ostracised by their community. The survivor had to resort to psychological therapy to help with his/her anxiety.*

> *A survivor, a public personality, openly admits to having plastic surgery, including breast enhancements. A hate page on Facebook called 'You Are Wanted' was created. The survivor's photos were uploaded on the said page, without the survivor's consent. The survivor received at least 30 hateful comments, such as: - "You this fucking slut……Prostitute to the max. You this fucking ugly bitch. Fuck off, I think your pussy must be like a big hole. Obviously you did surgery because you are not beautiful enough but still you became uglier. Poor girl. Ugly cunt, if you suicide one day it will be the best day of my life;" "So what if she's 100% fake? I'd still bang her hard!;" "You talk like you are sucking a cock, don't bullshitlah;" "Stfu, fake plastic bitch…..you talk too much."*

> *A survivor expressed his/her religious opinion, which was captured in an article that gave readers the impression that the survivor claimed that God was created by vibrations. The article had attracted more than 700 hateful comments, such as, "Ambik dia berlakon dalam tanah kubur….bagi dia rasa sikit macamana keadaan orang macam dia bila tiba hari kematian…kot kot dia insaf;" "Babi punya babi gemuk ni…dah boleh jatuh munafik dasar babi gemuk ni;" "Cibai anak babi la ko ni…apalah nasib mak bapak yang melahirkan ko ni…..mesti dia kecewa lahirkan anak babi macam ni….semua ni usaha-usaha memesongkan akal orang Islam la ni sebab-sebab dia buat kenyataan macam ni…kimak punya kafir sesat…tembak je bagi mampos..haram jadah…muka dahlah macam syaitan….puiii;" "Bila la dia nak mati?;" "If it were up to me, I would have chopped off this [name of the survivor] head already...traitor to the religion and destroyer of the faith of Muslims in these times".*

In 2013, someone posted a video of the survivor singing in a competition, on Facebook and tagged him/her. It attracted more than 70 comments mocking his/her singing and hateful comments, such as, "Oh yeah? …..what action are you going to take? Stfu? Yo….you are the one who should stfulah….still writing a fucking long essay…don't think you are so goodlah…kid, you're messing with the wrong person…don't let me find you in [……..]! Mark my words;" "Eh, since this video is posted on FB, I got my right to comment…and [person who uploaded the video's name] is my friend and this video is posted by my friend….so? This is my business also…..Yo and you warned me to watch my back and called me DUDE? Well, listen BABE! You got a big mouth….just can load four guys' cum in it…..so what I advise you …..go back, sit your ass down..and think who are you messing up with." The survivor claimed that he/she suffered depression for more than a year.

In 2013, a survivor, a part-time dog trainer, was criticised over a video showing him/her walking and bathing his/her dogs; the video was shared without the survivor's permission. The person who reposted the video changed the title of the video to "Video Menghina Islam Satu Hari di Hari Raya." According to the survivor, he/she received death threats via text messages of more than 40 hateful comments, such as, "Kepala hotak kau…kalau aku jumpa kau….aku bunuh terus. Buat malu orang Islam je, Kau ni aku layak perangi atas jihad demi menegakkan agama Islam. Aku perangi kau! Aku perangi kau!! Takbir;" "Hahahaha….I wish I could behead you. Typical, non-Muslim;" "Dengan nama Allah, kerajaan bagi greenlight bunuh, akulah orang pertama akan offer bunuh dia ni;" "Kasi bunuh ini perempuan, memalukan kaum, bangsa dan agama. Sesat;" "DARAH ORANG YANG MENGHINA ISLAM NI, HALAL UNTUK DIBUNUH!" "Orang yang hina Islam macam ni sepatutnya kena tembak je bagi mampus"; "Best example of a lonely attention seeking bitch!!! A swab test on her mouth would probably prove that she blows these dogs…haha."

1.61 Finally, it is clear in the relevant laws in the UK, Ireland and Australian that the test to be applied to prove harassment, stalking, grossly offensive communication, or menacing comments, is an objective one. Sections 1(2), 4(2), 4A of the UK Protection of Harassment Act 1997, section 10(2)(b) of the Irish Non-Fatal Offences Against the Person Act 1997 and section 474.17 of the Criminal Code 1995, states that what amounts to the said offence is if a reasonable person in possession of the same information would regard the said conduct or communication as an offence.

1.62 Both sections 211 and 233(1) of the CMA 1998 is silent on this and neither has the Courts provided an interpretation as to the test that is required to prove the offences in these sections.

1.63 In view of the comparative differences in the way the CMA 1998 and the laws in the UK, Ireland, and Australia, deal with cyberharassment and other forms of harmful cyber behaviour, it is desirable that a new offence of cyberharassment is introduced in section 233(1) of the CMA 1998, including a more detailed definition of the offence itself, key words in the offence, and the test to be applied.

1.64 Additionally, the requirement that the behaviour is persistent before it can be said to be an offence is important to set the threshold of seriousness of the offence. The punishment for offences in section 233(1) of the CMA 1998 is a rather hefty fine of RM50,000 or one year imprisonment or both; as such, the offence should include a corresponding threshold of gravity.

1.65 In the same vein of setting a threshold of seriousness to the offence, to ensure that provision that the CMA 1998 strikes a balance between freedom of expression and the need to ensure the Internet continues to be an empowering space, it would be beneficial

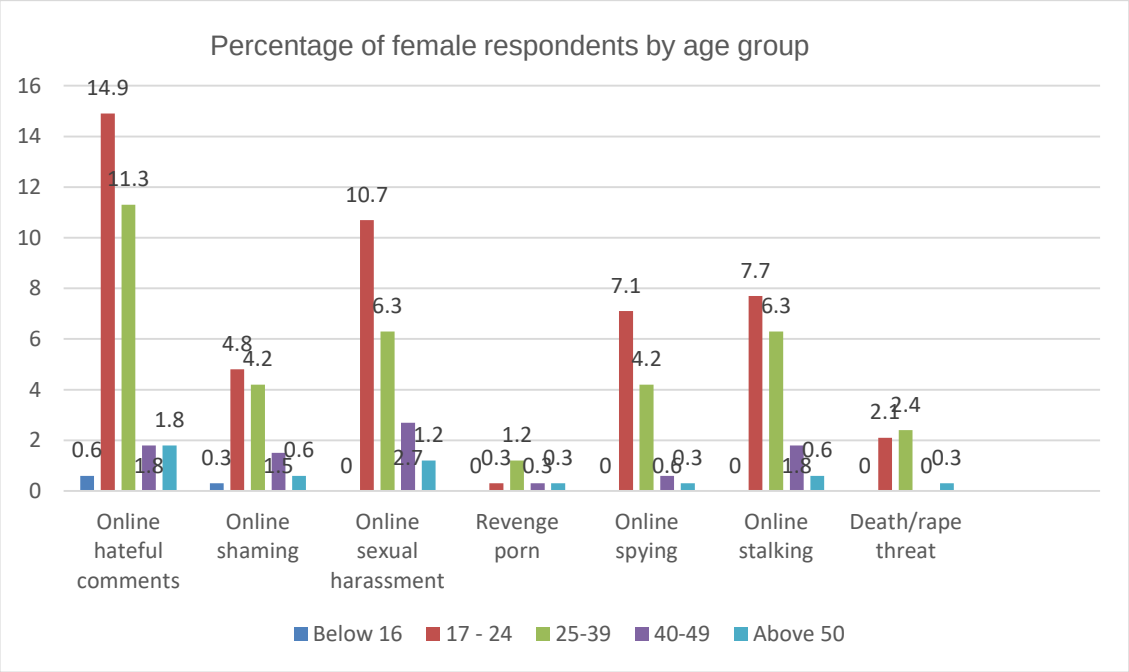
if sections 211 and 233(1) are amended to include “grossly” to offensive communication, thereby making only grossly offensive communication an offence. This is consistent with the objectives of the CMA 1998 (as stated in section 3(2)), which are to, *inter alia*, promote a civil society where information-based services will provide the basis of continuing enhancements to quality of work and life; and regulate for the long-term benefit of the end user.

1(a) Should a more specific offence of cyberharassment, including detailed definition of the offence itself, key words in the offence, and the test to be applied, be introduced in section 233(1) of the Communications and Multimedia Act 1998? 1(b) If such an offence of cyberharassment is introduced, should it include “persistent behaviour” as an element of the offence? 1(c) Should sections 211 and 233(1) be amended to include the word “grossly” to offensive communication?

ISSUE 2: WHETHER THE CURRENT LAW IS SUFFICIENT TO ADDRESS ONLINE SEXUAL HARASSMENT

2.1 Integral to the issue of cyberharassment discussed in Issue 1 is the growing problem of online sexual harassment. According to the Survey conducted by the PeopleACT, online sexual harassment was the second highest type of cyberharassment experienced by the respondents - a total of 89 respondents stated that they have been sexually harassed online.[58] In addition, the data showed that twice as many women (20.9 percent) experienced online sexual harassment than men (9.8 percent).

2.2 Also, it is observed that women of all ages were vulnerable to online sexual harassment - online sexual harassment was the highest type of cyberharassment for women ages between 17 and 24 years and 40 and 49 years selected and the second highest for women between the age of 25 and 39 years.



Disaggregated data for female respondents by age group of the types of online harassment they have experienced

2.3 In Malaysia, the Employment Act 1955 was amended by the Employment (Amendment) Act 2012 to include sexual harassment as an offence. Section 2 of the 1955 Act defines "sexual harassment" as "any unwanted conduct of a sexual nature, whether verbal, non-verbal, visual, gestural or physical, directed at a person which is offensive or humiliating or is a threat to his well-being, arising out of and in the course of his employment".

2.4 Significantly, section 81G provides that Part XVA on 'sexual harassment' applies to every employee employed under a contract of service irrespective of the wages of the employee. This provision is important as it extends the protection to all employees regardless of salary (paragraph 1 of the First Schedule limits the application of the Employment Act 1955 to employees earning RM2,000.00 or less).

2.5 An employee may file a sexual harassment complaint against an employee or an employer and *vice versa* (section 81A). Sections 81B to 81E sets out the procedure of

[58] Online sexual harassment was defined as being called obscene names, receiving unwanted pornographic materials or unwanted sexual images.

an inquiry into a sexual harassment complaint. It is an offence if an employer fails to carry out an inquiry into complaints of sexual harassment.

2.6 Thus far, there are no reported cases under Part XVA of the Employment Act 1955.

Tort of harassment

2.7 In addition to the Employment Act 1955, in November 2016, in the case of *Mohd. Ridzwan Bin Abdul Razak v Asmah Binti Hj. Mohd. Nor*,[59] the Federal Court undertook some "judicial activism exercise and decided to import the tort of harassment into the Malaysian legal and judicial system, with sexual harassment being part of it".[60] The Federal Court, in upholding the decision of the High Court and the Court of Appeal held:

- That sexual harassment are "unwelcome, taking the form of verbal and even physical, which include sexual innuendos, comments and remarks, suggestive, obscene or insulting sounds, implied sexual threats, leering, ogling, displaying offensive pictures, making obscene gestures etc. These overtures all share similar traits, in that they all have the air of seediness and cause disturbance or annoyance to the victim";[61]
- The standard of proof in this instance is balance of probabilities;
- In this case, it has been proven that there is persistent and deliberate course of unreasonable and oppressive conduct targeted at the respondent, calculated to cause alarm, fear and distress to that person;[62]
- Sexual harassment is a very serious misconduct and in whatever form it takes, cannot be tolerated by anyone. In whatever form it comes, it lowers the dignity and respect of the person who is harassed, let alone affecting his or her mental and emotional well-being. Perpetrators who go unpunished, will continue intimidating, humiliating and traumatising the victims thus resulting, at least, in an unhealthy work environment.[63]

2.8 The elements of the tort of sexual harassment in *Mohd. Ridzwan Bin Abdul Razak* differed slightly from section 2 of the Employment Act 1955 – the former requires "persistent" course of conduct as an element of harassment. As pointed out above (in Issue 1), persistent conduct is a requisite element in many anti-harassment legislation in other jurisdictions. This requirement ensures that mere one-off comments would not be caught by the law.

Other jurisdictions

Hong Kong

2.9 In Hong Kong, in 2013, the Courts recognised the tort of harassment in the case of *Lau Tat Wai V. Yip Lai Kuen Joey.*[64] The parties met in March 2007 in a Japanese language class where they soon developed a romantic relationship. Four months later, the plaintiff tried to end the relationship with the defendant. From then on, the defendant sent malicious emails, nuisance calls, surveillance and intrusions of privacy towards the plaintiff and his family, friends, colleagues, superiors and neighbours. The defendant also lodged false police reports resulting in the plaintiff's wrongful arrest and debt collector tactics involving splashing paint at his home and putting up derogatory posters about him. As a result the plaintiff had to frequently change jobs and homes. At its extreme, he moved with his mother to a rented flat in Shenzhen to evade the defendant, *albeit* unsuccessfully – she found him and splashed red paint on the iron grille.

[59] Civil Appeal No. 01(f)-13-06/2013 (W).
[60] See para. 39.
[61] See para. 59.
[62] See para. 79.
[63] See para. 81.
[64] [2013] HKCFI 639; [2013] 2 HKLRD 1197; [2013] 3 HKC 361; HCA 1466/2011 (24 April 2013)

2.10 The Court in this case defined 'harassment' to mean "a course of conduct by a person, whether by words or action, directly or through third parties, sufficiently repetitive in nature as would cause, and which he ought reasonably to know would cause, worry, emotional distress or annoyance to another person. This is not intended to be an exhaustive definition of the term but rather one that sufficiently encompasses the facts of the present case in order to proceed with a consideration of the law." The plaintiff was awarded special damages for his financial losses (loss of salaries, rental of outside premises and legal costs) as a result of the harassment; aggravated damages of HK$600,000 for the victim's hurt feelings, dignity and pride; exemplary damages of HK$200,000 as a punitive measure; and an injunction restraining the defendant from any further harassment of him and his family.

United Kingdom

2.11 In the UK, the civil tort of harassment can be found in section 3 of the Protection from Harassment Act 1997. Section 3 allows a victim to bring a civil action for harassment (as defined in section 1). Different from sections 2 and 4 of the 1997 Act, which are criminal proceedings, section 3 merely requires one act of harassment and anticipated further harassment; sections 2 and 4 requires a course of conduct.[65]

2.12 In addition, the civil remedies available under section 3 include damages, a restraining order and an injunction. Section 3(2) states that damages may be awarded for anxiety caused and any financial loss. In addition, a breach of an injunction or the restraining order by the defendant, the plaintiff may apply for a warrant of arrest (section 3(3)).

2.13 In a case concerning online sexual harassment, in *AMP v Persons Unknown*,[66] the claimant's mobile phone was stolen or lost in June 2008 and in the said phone contained digital images of her family and friends and images of an explicit sexual nature taken by her boyfriend for personal use. Subsequently, the digital images were uploaded to a free online media hosting service and her name and Facebook profile was attached to these images. The claimant was then contacted via Facebook from a person named Nils Henrik-Derimot threatening to expose her identity and to post the images widely online and tell her friends about the images if she did not add him as a friend on Facebook. She ignored the threat. A couple of months later, the images were uploaded to a Swedish website that hosts BitTorrent files, and the claimant's name was appended to each image, facilitating online search engines. Since then the images have been downloaded an unknown number of times by unknown persons. The claimant claimed amongst others an injunction under section 3 of the 1997 Act, to restrain an actual or expected breach of the 1997 Act. The Court considered the case amounted to harassment as there has been conduct on at least two occasions targeted at the claimant that were calculated to cause alarm and distress and would be oppressive and unacceptable. The Court granted an interim injunction to prevent the distribution of the digital images either by downloading from a website or by the use of BitTorrent.

Singapore

2.14 In 2014, Singapore passed the Protection from Harassment Act 2014, which created two harassment offences:

- Section 3 of the said Act makes it an offence for any person, with the intent to cause harassment, alarm, or distress to another person (a) use any threatening, abusive, or insulting words or behaviour; or (b) make any threatening, abusive, or insulting communication; causing the other person or any other person harassment, alarm, or

[65] CPS Legal Guidance on Stalking and Harassment, <http://www.cps.gov.uk/legal/s_to_u/stalking_and_harassment/#a10b> accessed 27 March 2017.
[66] [2011] EWHC 3454 (TCC) (20 December 2011).

distress. The punishment for this offence is a fine not exceeding SGD5,000 or imprisonment not exceeding six months or both;

- Section 4 of the 2014 Act makes it an offence for any person who uses any threatening, abusive, or insulting words or behaviour; or makes any threatening, abusive, or insulting communication, which is heard, seen, or otherwise perceived by any person likely to be caused harassment, alarm, or distress. The penalty for this offence is a fine not exceeding SGD5,000. Defences available for this offence include that he or she had no reason to believe that the words, behaviour, or communication would be heard, seen or otherwise perceived by the victim, or that his conduct was reasonable. Section 4 does not require any intention on the part of the accused.

2.15 Remedies available include damages, protection order, and an expedited protection order.

2.16 Section 14 of the Protection from Harassment Act 2014 abolished the tort of harassment, stating that no civil action for common law tort of harassment should be brought after 15 November 2014.

2.17 In June 2016, the first person was convicted under section 4 of the Protection from Harassment Act 2014. Lai Zhi Heng was in a brief sexual relationship with the victim in 2013. After they broke up, he threatened to go to her home if she did not send him a nude picture of her – she complied. He then threatened to show that nude picture to her mother and as a result she sent him a further 30 nude pictures of herself. Subsequently, when she ignored him, he printed her nude pictures and pasted them on the walls of her apartment building and posted nude photographs of her on her school's social media platform.[67] The Court convicted him for harassment and sentenced him to 12 months imprisonment.[68]

Analysis

2.18 Although all Internet users face sexual harassment, women are more likely to be victims because of their gender. This is evident from the data of the Survey and findings of the UN (see above).

2.19 The sexual harassment laws (both the Employment Act 1955 and the tort) in Malaysia may be sufficiently flexible to include online sexual harassment. It is arguable that the current legal provisions could cover potential online sexual harassment acts such as "sending unwanted sexual messages, gender-humiliating comments, sexual remarks, sending sexually explicit pictures, requests for company, sexual favours and comments about dress".[69]

2.20 However, it should be noted that the definition of sexual harassment in the Employment Act 1955 extends only to acts "arising out of and in the course of his employment". This limitation excludes a whole host of online sexual harassment incidents, which occur outside the employment setting. For example, in all the incidents captured by the

[67] Elena Chong, 'Man first to be convicted for unlawful stalking', *Straits Times*, 2 June 2016, <http://www.straitstimes.com/singapore/courts-crime/man-first-to-be-convicted-under-protection-from-harassment-act-for-stalking> accessed 30 March 2017

[68] Elena Chong, 'Man jailed 12 months for unlawful stalking and rash act causing hurt', *Straits Times*, 17 June 2016, <http://www.straitstimes.com/singapore/courts-crime/man-jailed-12-months-for-unlawful-stalking-and-rash-act-causing-hurt> accessed 30 March 2017.

[69] Recommended citation: Mohamed Chawki, Yassin el Shazly, Online Sexual Harassment: Issues & Solutions 4 (2013) JIPITEC 2, para 71. <https://www.jipitec.eu/issues/jipitec-4-2-2013/3742/harassment.pdf> accessed 30 March 2017.

PeopleACT, complaints of online sexual harassment took place outside the bounds of employment:

> *A 30-year-old survivor has been receiving images with sexual content at least once a couple of months via Whatsapp from a person, who is not his/her co-worker. The survivor feels extremely uncomfortable receiving these messages.*

> *In 2013, a survivor who appeared in a video supporting a political party received rape and death threats on Facebook. The survivor's photos were circulated and the comments received include, "To pay Mat Rempit to gang rape her soon….if I could find out where she is now;" "Talk to my cock." "One day, Bangla will rape her;" "F(uck) her kow kow (badly);" "One day this bitch kena (get) snatch beside the road, I sure won't help her out, lol, since she likes BN rempit so much;" "I think this bitch will kena (get) rape very soon;" "Wash your cunt first. So fucking smelly."*

> *After refusing to go on a date with A, a survivor persistently received violent and obscene text messages via Whatsapp voicemail from A. Two of the messages read, "Aku penggal kepala kau. Kepala anak sulung kau aku belah. Kau sundal. Anak kedua kau babi" and "Aku lapah kau. Jantung kau aku rentap" from the man. A told the survivor that A had published pornographic photos of the survivor on social media and A was monitoring his/her movement outside his/her house.*

> *In 2012, the survivor met B on Facebook who introduced himself as a 30-year-old Indian heir from Kerala working as an engineer in a company. Although the survivor told B that he/she was not interested in having a relationship, B insisted on waiting for him/her. Subsequently, B told the survivor that he was coming to Malaysia and wanted to meet him/her alone. B told the survivor that he was living in a hotel close to the survivor's house. The survivor became worried and immediately tried to discourage B by telling him that they would never communicate again. B got upset and started calling the survivor on the phone numerous times. One time, when the survivor answered B's call, he started revealing his sexual fantasies of the survivor. The survivor blocked B from his/her phone contact list and Facebook.*

> *In 2013, the survivor received hateful messages on Twitter about his/her appearance, weight, hair, virginity, etc. from anonymous accounts. There was one which said, "I know what you used to do with your ex [boyfriend]."*

2.21 The judgement of the Federal Court in *Mohd. Ridzwan Bin Abdul Razak* would appear to encompass sexual harassment outside the work place – the Federal Court, in finding that there was sexual harassment stated that "the ingredients of sexual harassment….namely, the existence of a persistent and deliberate course of unreasonable and oppressive conduct targeted at another person…, calculated to cause alarm, fear and distress to that person". There was no mention that the harassment should take place in the course of employment or that it had created a hostile working environment. As such, it is arguable that the tort of harassment as defined by the Federal Court is sufficient to encompass not only online sexual harassment that occurs outside the workplace but also generally online harassment and other forms of harmful cyber behaviour.

2.22 Looking at UK, Hong Kong, and Singapore, cases of online sexual harassment were prosecuted using general laws prohibiting harassment. A brief summary of the elements of the different provisions in a selected number of jurisdictions:

Section 233 of the CMA 1998	**Sections 4 & 7 of the UK Protection from Harassment Act 1997**	**Sections 3 & 4 of the Singapore Protection from Harassment Act 2014**
Section 233(1) - By means of network facilities/services/application services - Knowingly makes, creates, or solicits, and initiates transmission - Any comment, request, suggestion, or other communication - Which is obscene, indecent, false, menacing, or offensive - With intent to annoy, abuse, threaten, or harass, another person *Section 233(2)* - Knowingly initiates a communication - Whether continuously, repeatedly, or otherwise - With intent to annoy, abuse, threaten, or harass any person	- Pursue a course of conduct - Which amounts to harassment (causing distress or alarming a person) - That he knows or ought to know amounts to harassment	*Section 3* - Intent to cause harassment, alarm, or distress - By any means - By using threatening, abusive, or insulting - Words, behaviour, or communication - Causing that person/ any other person - Harassment, alarm, or distress *Section 4* - By any means - Use any threatening, abusive, or insulting - Words, behaviour, or communication - Which is seen, heard, or otherwise perceived by any person - Likely to cause harassment, alarm, or distress.

2.23 It is observed that in defining the elements of harassment, laws in the UK do not require that the communication, words or behaviour to be obscene, indecent, false, menacing or offensive. Instead, harassment is proven when the act, words, communication, or behaviour causes or is likely to cause harassment, alarm, or distress. This is comparable with the definition provided by the Federal Court in the case of *Mohd. Ridzwan Bin Abdul Razak*. In Singapore, the words, behaviour or communication must be threatening, abusive, or insulting.

2.24 In addition, in UK and Singapore, the remedies available include protection orders or restraining orders and damages. These remedies are not available under the Employment Act 1955 or sections 211 and 233(1) of the CMA 1998. Damages and an injunction are available if the course of action pursued is by way of a tort of harassment. With the nature of online sexual harassment where comments and postings have a high potential of going viral, victims/survivors of online sexual harassment and harassment generally would benefit more from speedy and inexpensive remedies.

2.25 Therefore, it is perhaps timely that a specific offence of sexual harassment or a general offence of harassment, akin to the Federal Court's definition in *Mohd. Rizwan bin Abdul Razak,* is codified in statute, to cover online and offline sexual harassment. In this regard, it is equally pertinent that the same legal provision establishes clear remedies such as protection orders and expedited protection orders.

2 (a) Does the current law (statute and case law) adequately addresses the problem of online sexual harassment (inside and outside the workplace), including available legal remedies?

2 (b) If the answer to the above is no, then should a specific offence of online sexual harassment be introduced or should a more general offence of harassment be codified in statute?

ISSUE 3: WHETHER THE CURRENT LAW PROHIBITING OBSCENE PUBLICATIONS IS SUFFICIENT TO TACKLE CYBERHARASSMENT AND OTHER HARMFUL CYBER BEHAVIOUR

3.1 One particular form of cyberharassment that the Survey respondents face, is lewd and obscene comments, comments relating to the victim/survivor's private parts, and revenge porn; revenge porn is the posting or distributing of intimate photographs or images of the victim/survivor. According to the Survey, 77.4 percent of respondents regard revenge porn[70] as online violence. However, only 12 out of 522 respondents have experienced revenge porn.

3.2 Some examples of aforementioned incidents collated by the PeopleACT include:

After refusing to go on a date with A, a survivor persistently received violent and obscene text messages via Whatsapp voicemail from A. Two of the messages read, "Aku penggal kepala kau. Kepala anak sulung kau aku belah. Kau sundal. Anak kedua kau babi" and "Aku lapah kau. Jantung kau aku rentap" from the man. A told the survivor that A had published pornographic photos of the survivor on social media and A was monitoring his/her movement outside her house. The survivor said that he/she was receiving these messages a couple of times a day for six months. He/she quickly deactivated his/her Facebook account, relocated his/her family and changed his/her phone number. Even then, he/she continued to receive anonymous phone calls which he/she suspected were coming from A.

In 2013, a survivor who appeared in a video supporting a political party received rape and death threats on Facebook. The survivor's photos were circulated and the comments received include, "To pay Mat Rempit to gang rape her soon….if I could find out where she is now;" "Talk to my cock." "One day, Bangla will rape her;" "F(uck) her kow kow (badly);" "One day this bitch kena (get) snatch beside the road, I sure won't help her out, lol, since she likes BN rempit so much;" "I think this bitch will kena (get) rape very soon;" "Wash your cunt first. So fucking smelly."

[70] Revenge porn is defined in the Survey as "when someone threatens to upload sexually explicit photos of you as revenge".

In 2013, a survivor, a part-time dog trainer was criticised over a video showing him/her walking and bathing his/her dogs; the video was shared without the survivor's permission. The person who reposted the video had changed the title of the video to "Video Menghina Islam Satu Hari di Hari Raya." According to the survivor, he/she received death threats via text messages and more than 40 hateful comments, such as, "Kepala hotak kau…kalau aku jumpa kau….aku bunuh terus. Buat malu orang Islam je, Kau ni aku layak perangi atas jihad demi menegakkan agama Islam. Aku perangi kau! Aku perangi kau!! Takbir;" "Hahahaha….I wish I could behead you. Typical, non-Muslim;" "Dengan nama Allah, kerajaan bagi greenlight bunuh, akulah orang pertama akan offer bunuh dia ni;" "Kasi bunuh ini perempuan, memalukan kaum, bangsa dan agama. Sesat;" "DARAH ORANG YANG MENGHINA ISLAM NI, HALAL UNTUK DIBUNUH!" "Orang yang hina Islam macam ni sepatutnya kena tembak je bagi mampus"; "Best example of a lonely attention seeking bitch!!! A swab test on her mouth would probably prove that she blows these dogs…haha."

A survivor, a public personality, openly admits to having plastic surgery, including breast enhancements. A hate page on Facebook called 'You Are Wanted' was created. The survivor's photos were uploaded on the pages, without his/her consent. The survivor received at least 30 hateful comments, such as: - "You this fucking slut……Prostitute to the max. You this fucking ugly bitch. Fuck off, I think your pussy must be like a big hole. Obviously you did surgery because you are not beautiful enough but still you became uglier. Poor girl. Ugly cunt, if you suicide one day it will be the best day of my life;" "So what if she's 100% fake? I'd still bang her hard!; ""You talk like you are sucking a cock, don't bullshitlah;" "Stfu, fake plastic bitch…..you talk too much."

3.3 For these incidents, two legislation may be relevant – section 292(a) and 509 of the Penal Code and sections 211 and 233(1) of the CMA 1998 – all three provisions deal with obscene or indecent communications.

Section 292(a) of the Penal Code

3.4 Section 292(a) of the Penal Code makes it an offence for any person to amongst others, distribute, publicly exhibit or in any manner puts into circulation, or for purposes of distribution, public exhibition or circulation any obscene book, pamphlet, paper, drawing, painting, representation of figure or any other obscene object whatsoever. The punishment is imprisonment that may extend to three years or a fine or both. Section 292(a) makes an exception for objects of artistic and religious content.[71]

3.5 Section 292(a) does not require intention or knowledge on the part of the accused. In *Mohamad Ibrahim v PP,*[72] it was held that the accused in this case was incapable of reading or writing in English and could not comprehend the book entitled 'Tropics of Cancer' as an obscene book is immaterial. The mere possession of such obscene books or materials makes the persons strictly liable.

3.6 One of the essential ingredients of the offence in section 292(a) is that the object in question must be obscene. What amounts to obscene was examined in *Mohamad Ibrahim v PP*[73] where the Courts followed the test of obscenity laid out in the UK case of *R v Hicklin*[74] i.e., "whether the tendency of the matter charged as obscenity is to deprave and corrupt those whose minds are open to such immoral influences, and into whose hands a public of this may fall".

[71] Mohd. Rizal Mat Yusuf v PP [2009] 3 CLJ 798, at 817.
[72] [1963] 1 MLJ 289.
[73] [1963] 1 MLJ 289.
[74] (1868) LR 3 QB 360.

3.7 Cases under section 292(a) of the Penal Code illustrate that the Courts consider sexual acts as obscene objects within the meaning of section 292(a). For example, in *Public Prosecutor v. Vun Tain Yin & Anor,*[75] the Court held that sexual acts, which were filmed, produced, sold and distributed by the first and second respondents, into video cassettes, amounted to obscene objects within the meaning of section 292(a) of the Penal Code. The High Court increased the punishment from MYR600 to two months imprisonment on the account of the "seriousness of the offence and the moral implications of it as well as public interest". Similarly, in *Mohd Rizal Mat Yusuf v. PP,*[76] the Court regarded the VCD that contained scenes of sexual activities between Rizal, a flight attendant, and a fellow female flight attendant and other females including his wife, were obscene and amounted to pornography.

3.8 Thus far, there are no reported cases under section 292(a), which relates to the transmission of obscene objects via social media or the like and as such it cannot be said for certain that section 292(a) of the Penal Code can be used to tackle cyberharassment cases. However, the case of *Mohd Rizal Mat Yusuf v. PP*[77]where "any object whatsoever" was interpreted by the Courts to include "visual recordings such as are contained in a video compact disc," suggests that the Courts are open to extending section 292(a) to situations involving cyber enabled technology.

Section 509 of the Penal Code

3.9 Section 509 of the Penal Code could also be used to tackle the problem of cyberharassment, particularly if it involves obscene communications. Section 509 states that any person who intends to insult the modesty of any person who "utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen by such person, or intrudes upon the privacy of such person", is guilty of an offence. The punishment for this offence is imprisonment for a term which may extend to five years or a fine or both.

3.10 As to what amounts to "intrudes upon the privacy", it is said that the accused must intend to insult the modesty of such person whose privacy is intruded upon. Also, it is possible to intrude on the privacy of a person in a public place.[78]

3.11 In *Maslinda binti Ishak v Mohd Tahir bin Osman & 3 Ors,*[79] the appellant was arrested at a night club by officers from RELA (*Angkatan Relawan Rakyat Malaysia*) and JAWI (*Jabatan Agama Islam Wilayah Persekutuan*). The appellant together with other persons arrested were put in a truck and driven to Taman Maluri, Cheras. En route, the appellant requested the RELA and JAWI officers' permission to use the toilet facilities but was disallowed. Instead the said officers scolded her and told her to urinate in the truck. Consequently, she asked her friends to encircle her with a shawl in order to ease herself. At that moment, the first defendant suddenly opened the door of the truck, rushed in, pulled down the shawl and proceeded to take numerous photos of the appellant in a squatting position urinating. As a result, the appellant was thoroughly humiliated. The first defendant was prosecuted under section 509 of the Penal Code and was sentenced to four months imprisonment.

[75] [1986] 1 CLJ 94.
[76] [2009] 3 CLJ 798.
[77] [2009] 3 CLJ 798.
[78] Annotated Statues of Malaysia, 2014, Issue 118, Vol. 5, at pg. 2505.
[79] [2009] 1 LNS 891.

3.12 Other reported cases under section 509 of the Penal Code involve insulting the modesty of the victim by asking the victim to take off her clothing and taking nude photographs of the victim.[80]

3.13 To date, there are no reported cases under section 509 of the Penal Code that relates to cyberharassment or other harmful cyber behaviour.

Sections 211 and 233(1) of the CMA 1998

3.14 Apart from the provisions in the Penal Code, sections 211 and 233(1) of the CMA 1998 are also relevant. Elaborated above (in Issue 1), these provisions make it an offence if a person using a content applications service or a network facilities or network service or applications service, provides, makes, creates, solicits, or initiates the transmission of, any comment, request, suggestion or other communication which is obscene, with intent to annoy, abuse, threaten or harass another person.

3.15 Like the Penal Code, the CMA 1998 does not define the word 'obscene' and cases tried under the CMA 1998 have not laid out a definitive interpretation either. In *PP v Chan Hon Keong*[81] (see above for facts), the Sessions court looked at the ordinary dictionary meaning of the word "obscene" to mean "offensively or repulsively indecent, especially by offending accepted sexual morality. 'Obscenity' is the state or quality of being obscene." The Sessions court judge also referred to the Indian case of *Ranjit D Udeshi v State of Mahrashtra*[82] where the Indian courts held that the word obscene "denotes the quality of being obscene which means offensive to modesty or decency, lewd, filthy and repulsive. It cannot be denied that it is an important interest of society to suppress obscenity. There is of course, some difference between obscenity and pornography in the latter denotes writing, pictures, etc. intended to arouse sexual desire while the former may include writings, etc. not to do so but have tendency. Both of course offend against public decency and morals but pornography is obscenity in a more aggravated form." The court subsequently held that the phrase "*kepala butuh*" is an obscene phrase as generally understood by the public; this is because the words denote the private parts of a man and a comment using those words directed at the Sultan of Perak contains obscene elements and is intended to hurt the Sultan of Perak.

3.16 A more detailed definition of the words "indecent" and "obscene" can be found in the non-binding and voluntary Content Code. Part 2 of the said Code defines the said as follows:[83]

- Indecent content - material which is offensive, morally improper and against current standards of accepted behaviour. This includes nudity and sex. Sex and nudity cannot be shown unless approved by the Film Censorship Board;
- Obscene content – material that gives rise to a feeling of disgust by reason of its lewd portrayal and is essentially offensive to one's prevailing notion of decency and modesty. There is every possibility of such content having a negative influence and corrupting the mind of those easily influenced. The test of obscenity is whether the Content has the tendency to deprave and corrupt those whose minds are open to such communication. Any portrayal of sexual activity that a reasonable adult considers explicit and pornographic; portrayal of sex crimes, including rape or attempted rape and statutory rape; bestiality; child pornography; sexual degradation of men, women, or children; sexual violence, are prohibited (whether animated or consensual).

[80] *Mohd Hanafi Ramly v. PP*, [2012] 2 CLJ 326.
[81] [2012] 5 LNS 184.
[82] [1965] AIR (SC) 991; [1965] 1 SCR 65.
[83] <http://cmcf.my/onlineversion/part2-guidelines-content#1.0> accessed 17 March 2017.

Other jurisdictions

United Kingdom

3.17 The relevant portion (to Issue 3) of the Malicious Communications Act 1998 is the offence of sending to (a) a person a letter or other article which conveys a message which is ***indecent***… (emphasis added) or (b) any other article which is, in whole or part, indecent…, and in sending it is that it should, so far as falling within paragraph (a) and (b) above, cause distress or anxiety to the recipient or to any other person to whom he intends that it or its contents or nature should be communicated.

3.18 Section 127(1) of the Communications Act 2003 is also relevant as it makes it an offence if a person sends by means of a public electronic communications network a message or other matter that is grossly offensive or of an ***indecent, obscene*** (emphasis added) or menacing character; or causes any such message or matter to be so sent.

3.19 For cases under section 1 of the Malicious Communications Act 1988 or section 127 of the Communications Act 2003, CPS 'Guidelines on prosecuting cases involving communications sent via social media', sets out the approach that prosecutors should take when making decisions in relation to cases where it is alleged that criminal offences have been committed by the sending of a communication via social media. Apart from the two stage test,[84] the said Guidelines recommends prosecutors should also weigh the effect on the victim in cases of indecent and obscene communications sent via social media, particularly where:

- There is a hate crime element to the communications;
- The victim was at the time a person serving the public;
- There are coordinated attacks by different people or there is a campaign of abuse or harassment against the victim, sometimes referred to as "virtual mobbing";
- The victim is targeted in response to the victim reporting a separate criminal offence;
- A person convicted of a crime subsequently contacts the victim of that crime, or their friends or family;
- The offence is repeated.

3.20 In the UK, the Courts effectively encapsulated the link between obscene and indecency stating both obscenity and indecency offend "against the recognised standards propriety….indecent being at the lower end of the scale and obscene at the upper end of the scale".[85]

3.21 Specifically to obscenity, in *Gibson and Sylveire,*[86] Lord Lane CJ held that "there are two broad types of offence involving obscenity… one involving corruption of public morals… and the other involve an outrage on public decency, whether or not public morals are involved".

3.22 As to what amounts to obscenity, depending on the article or activity,[87] the test can be found either in statute or case law:

- Section 1 of the Obscene Publications Act 1959[88] states that "an article shall be deemed to be obscene if its effect or (where the article comprises two or more distinct

[84] Generally, prosecution may start if a case satisfies the test set out in the Code for Crown Prosecutors. This test has two stages: - (a) the requirement of evidential sufficiency; and (b) consideration of the public interest. Evidential stage – a prosecutor must be satisfied that there is sufficient evidence to provide a realistic prospect of conviction. It is an objective test based upon the prosecutor's assessment of the evidence. If a case does not pass this stage, the case must not proceed. But, even if the evidential stage is satisfied, the prosecutor must consider whether the prosecution is in the public interest – public interest stage.

[85] *R v Stanley* [1965] 1 All ER 1035.

[86] [1990] 2 QB 619.

[87] The Obscene Publications Acts 1959 applies only to publications.

[88] <http://www.cps.gov.uk/legal/l_to_o/obscene_publications/> accessed 22 March 2017.

items) the effect of any one of its items is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it";

- As for case law, in *Hamilton*[89] it was held that "it has to be proved both that the act is of such a lewd, obscene, or disgusting character and that it outrages public decency. (i) an obscene act is an act which offends against recognised standards of propriety and which is at a higher level of impropriety than indecency; see *R v Stanley*. A disgusting act is one which fills the onlooker with loathing or extreme distaste or causes annoyance; *R v Choi*[90]*…* (ii) it is not enough that the act is lewd, obscene, or disgusting and that it might shock people; it must, as Lord Simon made clear in the *Knuller*[91] case, the of such a character that it outrages minimum standards of public decency as judged…in a contemporary society. For the offences of obscenity and indecency, it is not necessary to show that any person was actually disgusted".[92]

3.23 In addition to the above, the standard to be applied assumes equal importance - as Lord Wilberforce stated in *Director of Public Prosecutor v Whyte,* "the tendency to deprave and corrupt is not to be estimated in relation to some assumed standard of purity of some reasonable average man. It is the likely reader"[93]…. in an open and just multi-racial society. This means that what amounts to obscenity is whether it would deprave and corrupt a reasonable person living in an open and just multi-racial society, who is likely to be exposed to the said obscene communication.

3.24 Apart from the Malicious Communications Act 1988, the UK introduced a new criminal offence of disclosing private sexual[94] photographs and films without the consent of an individual who appears in them, with the intent to cause that individual distress in sections 33 to 35 of the Criminal Justice and Courts Act 2015.

3.25 Distress within the section must be intended and not merely because that it was a natural and probable consequence of the disclosure (section 33(8) of the 2015 Act). It is not an offence if disclosure is made to the individual in that photograph or film.

3.26 Defences available include, if the person reasonably believed that the disclosure was necessary for the purposes of preventing, detecting or investigating crime; the disclosure was made in the course of, or with a view to, the publication of journalistic material, and it was, or would be, in the public interest to do so; he or she reasonably believed that the photograph or film had previously been disclosed for reward, whether by the individual mentioned or another person, and he or she had no reason to believe that the previous disclosure for reward was made without the consent of the individual mentioned.

---

[89] [2007] EWCA Crim 2062.

[90] 7 May 1999, unreported in The Law Commission Consultation Paper No 193, 'Simplification Of Criminal Law: Public Nuisance And Outraging Public Decency, <http://www.lawcom.gov.uk/wp-content/uploads/2015/06/cp193_public_nuisance.pdf> accessed 22 March 2017.

[91] *Knuller (Publishing, Printing and Promotions) Ltd v DPP,* [1073] AC 435, [1972] 3 All ER 898.

[92] *R v Lunderbach* [1991] Crim LR 784 (CA) and *R v Mayling* [1963] 2 QB 717.

[93] [1972] 2 All ER 12.

[94] Section 35(3) defines a photograph or film is "sexual" if - (a)it shows all or part of an individual's exposed genitals or pubic area; (b)it shows something that a reasonable person would consider to be sexual because of its nature; or (c)its content, taken as a whole, is such that a reasonable person would consider it to be sexual". Section 4 states that "Subsection (5) applies in the case of - (a)a photograph or film that consists of or includes a photographed or filmed image that has been altered in any way, (b)a photograph or film that combines two or more photographed or filmed images, and (c)a photograph or film that combines a photographed or filmed image with something else". Section 5 states that "the photograph or film is not private and sexual if - (a)it does not consist of or include a photographed or filmed image that is itself private and sexual; (b)it is only private or sexual by virtue of the alteration or combination mentioned in subsection (4), or (c)it is only by virtue of the alteration or combination mentioned in subsection (4) that the person mentioned in section 33(1)(a) and (b) is shown as part of, or with, whatever makes the photograph or film private and sexual".

3.27 According to the CPS, examples of this offence usually involve an adult ex-partner uploading onto the Internet intimate sexual images of the victim with the intent of causing the victim humiliation of embarrassment.[95]

Australia

3.28 Like the UK Criminal Justice and Courts Act 2014, revenge porn is tackled using the Summary Offences Act 1966. In the state of Victoria, sections 41DA and 41 DB of the Summary Offences Act 1966 make it an offence for a person to "intentionally distribute an intimate image of another person (B) to a person other than B; and the distribution of the image is contrary to community standards of acceptable conduct". A person who commits an offence against subsection (1) is liable to level seven imprisonment (two years maximum). This section does not apply if B is not a minor; and B had expressly or impliedly consented, or could reasonably be considered to have expressly or impliedly consented, to - (i) the distribution of the intimate image; and (ii) the manner in which the intimate image was distributed" (section 41DA(3)).These offences were introduced in 2014.

3.29 Section 41DB of the same Act also makes the threat[96] of distributing an intimate image an offence. The elements of the offence are if a person (A) makes a threat to another person (B) to distribute an intimate image of B or of another person (C); and the distribution of the image would be contrary to community standards of acceptable conduct; and A intends that B will believe, or believes that B will probably believe, that A will carry out the threat. The punishment if level eight imprisonment (one year maximum).

3.30 For the purposes of sections 41DA and 41DB, section 40 defines an "intimate image" as "a moving or still image that depicts: a person engaged in sexual activity; a person in a manner or context that is sexual; or the genital or anal region of a person or, in the case of a female, the breasts; and distribute" includes "(a) publish, exhibit, communicate, send, supply or transmit to any other person, whether to a particular person or not; and (b) make available for access by any other person, whether by a particular person or not".

Analysis

3.31 If it is suggested that the Penal Code and the CMA 1998 are used to prosecute alleged offenders in cyberharassment cases, then the crux of the action is the interpretation of the words "obscene", "indecent", and "modesty". Having said that, the test of what amounts to obscenity in Malaysia does not appear to be settled – on one hand, the 1960s case of *Mohamad Ibrahim v PP* adopted the test set out in the UK case of *R v Hicklin* of whether it tends to "deprave and corrupt those whose minds are open to such immoral influences, and into whose hands a public of this may fall"; whereas in the more recent case of *PP v Chan Hon Keong*, obscenity is defined as "offensive to modesty or decency, lewd, filthy and repulsive". And whilst the Content Code adopts the test in *R v Hicklin*, it remains a voluntary non-binding code.

3.32 The fragmented interpretation of the word 'obscene' leads to different interpretations of the word, depending on the understanding of the different authorities in charge of such cases. As we all have different levels of tolerance to lewdness and obscenity, it would be beneficial if a definition of obscene is clear and comprehensive where what amounts

[95] 'Violence Against Women and Girls: Crime Report 2015-16', UK Crime Prosecution Service (Sept 2016), <http://www.cps.gov.uk/publications/docs/cps_vawg_report_2016.pdf> accessed 2 February 2017.

[96] According to section 41DB(3), a threat may be made by any conduct and may be explicit or implicit.

to obscenity should be whether a reasonable person living in an "open and just multi-racial society"[97] would consider it so.

3.33 Contrast this with the position in UK where the Obscene Publications Act 1959 and case law have provided a comprehensive and cohesive test for what amounts to obscenity or indecency and the standard to which the concepts are measured against.

3.34 Similarly in Canada, the Canadian Supreme Court in the case of *R v Butler*,[98] applied the community standard of tolerance test to determine what amounted to obscenity – the test was "what Canadians would not tolerate being exposed to themselves, but with what they would not tolerate other Canadians being exposed to… What the community would tolerate others being exposed to on the basis of the degree of harm that may flow from such exposure. Harm in this context means that it predisposes persons to act in an anti-social manner, in other words, a manner which society formally recognizes as incompatible with its proper functioning. The stronger the inference of a risk of harm, the lesser the likelihood of tolerance".

3.35 In addition to the above, it is observed that Malaysia does not have comparable provisions to that of sections 33 to 35 of the UK Criminal Justice and Courts Act 2015 or sections 41DA and 41DB of the South Australian Summary Offences Act 1966 – the provisions in both these laws are suitable to deal with revenge porn, which essentially comprises the act of distributing or disclosing online, intimate images or photographs of another person without their permission.

3.36 As regards section 509 of the Penal Code, it may be difficult to use this provision to cyberharassment cases as section 509 requires the prosecution to prove that the accused intended to insult the modesty of the victim/survivor. This could be problematic in cyberharassment and other harmful cyber behaviour cases, particularly when the offender merely uploads intimate photographs of the victim/survivor with no intention to outrage the modesty of the victim/survivor but rather merely to embarrass or intimidate the victim/survivor.

3(a) Are current laws in Malaysia, as laid out in sections 292(a) and 509 of the Penal Code and sections 211 and 233(1) of the CMA 1998, adequately address revenge porn and similar harmful cyber behaviour?
3(b) In addition, should sections 292(a) and 509 of the Penal Code and sections 211 and 233(1) of the CMA 1998 be amended to include a statutory definition of the word 'obscenity'?
3(c) Should a comparable provision to sections 33 to 35 of the UK Criminal Justice and Courts Act 2015 or sections 41DA and 41DB of the South Australian Summary Offences Act 1966, be introduced in the Penal Code or the CMA 1998 to tackle revenge porn?

[97] Lord Wilberforce in *Director of Public Prosecutor v Whyte,* [1972] A.C. 849.
[98] [1992] 1 S.C.R. 452.

ISSUE 4: WHETHER CURRENT PENAL LAW ADEQUATELY ADDRESSES THREATS OF DEATH AND THREATS OF RAPE AND OTHER ABUSIVE COMMUNICATIONS MADE USING CYBER TECHNOLOGY

4.1 The use of threatening words seems to be occurring with more frequency, with the latest against a human rights defender, where it was reported that users of Facebook threatened to decapitate the survivor –"If it were up to me, I would have chopped off this [name of victim/survivor] head already...traitor to the religion and destroyer of the faith of Muslims in these times."[99] Unfortunately, these types of incidents are not unusual - other similar incidents collated by the PeopleACT include:

> *As a result of his/her personal details exposed online, the survivor received multiple death and rape threats and hateful comments from random people via his/her phone, Facebook and website between August to October/November 2011 - "I received random calls from people I do not know and SMS of death threats and people kept on sending me hate messages in my phone and Facebook with really horrible messages. Some wanted to rape me, some wanted to kill me slowly until I die a horrible death, some called me a whore and animal names, some even said I was born because my mom had sex with a dog… "*

> *Subsequent to posting an opinion on the "Allah-Herald" case on Facebook, the survivor was body-shamed, cursed, called a murtad, and the survivor received death threats such as "I know where you are"; "I know where to get you."*

> *Doctored image of [name of victim/ survivor A] and A's three sons, [name of victim/survivor B], and [name of victim/survivor C] kneeling in front of a man holding a large knife clad in a balaclava were sent twice to A's phone between October and November 2016. The image was accompanied by the message, "In the name of Allah, and the sanctity of the Islamic struggle in Malaysia, if you want to lose your head like in Syria, continue with your stupid work. I will ¬decapitate you, record it and spread it on You Tube. I know who you are, I know where you live and I know your family and children. This warning is from Islamic State Malaysia."*

> *In 2013, a survivor, a part-time dog trainer was criticised over a video showing him/her walking and bathing his/her dogs; the video was shared without the survivor's permission. The person who reposted the video had changed the title of the video to "Video Menghina Islam Satu Hari di Hari Raya." According to the survivor, he/she received death threats via text messages and more than 40 hateful comments, such as, "Kepala hotak kau…kalau aku jumpa kau….aku bunuh terus. Buat malu orang Islam je, Kau ni aku layak perangi atas jihad demi menegakkan agama Islam. Aku perangi kau! Aku perangi kau!! Takbir;" "Hahahaha….I wish I could behead you. Typical, non-Muslim;" "Dengan nama Allah, kerajaan bagi greenlight bunuh, akulah orang pertama akan offer bunuh dia ni;" "Kasi bunuh ini perempuan, memalukan kaum, bangsa dan agama. Sesat;" "DARAH ORANG YANG MENGHINA ISLAM NI, HALAL UNTUK DIBUNUH!" "Orang yang hina Islam macam ni sepatutnya kena tembak je bagi mampus".*

[99] Boo Su-Lyn, 'Siti Kasim gets death threats, branded 'destroyer' of Muslim faith after online interview', <http://www.themalaymailonline.com/malaysia/article/siti-kasim-gets-death-threats-branded-destroyer-of-muslim-faith-after-onlin#sthash.0q05sZz8.dpuf> accessed 23 March 2017.

In 2013, a survivor who appeared in a video supporting a political party received rape and death threats on Facebook. The survivor's photos were circulated and the comments received include, "To pay Mat Rempit to gang rape her soon….if I could find out where she is now;" "Talk to my cock." "One day, Bangla will rape her;" "F(uck) her kow kow (badly);" "One day this bitch kena (get) snatch beside the road, I sure won't help her out, lol, since she likes BN rempit so much;" "I think this bitch will kena (get) rape very soon;" "Wash your cunt first. So fucking smelly."

In 2015, a satirical video titled "Hudud: A Rice Bowl Issue" aimed at a light-hearted poke at the proposed Hudud bill, hosted by the survivor. The video was viewed more than 780,000 times and attracted hundreds of comments such as, "Those who insult the laws of Allah, their blood is halal for killing", "Wait til I rape you, woman", and "If I see you in front of me, I'll shoot you in the head." Access to these comments are no longer available as the survivor was forced to shut down his/her social media account due to the large number of hateful comments sent to him/her. According to close friends and family members, the survivor feared for his/her life and has since declined all interviews.

"Aku on the way ke rumah [name of survivor]. Aku akan masuk ikut bilik. Once aku dah atas katil, mohon siapa-siapa roger Pegawai Penyiasat Agama (PPA). Kalau kesiankan aku, roger esok malamlah. At least, aku boleh try dia dulu malam ini ," This was posted with a "feeling wonderful" Facebook emotion.

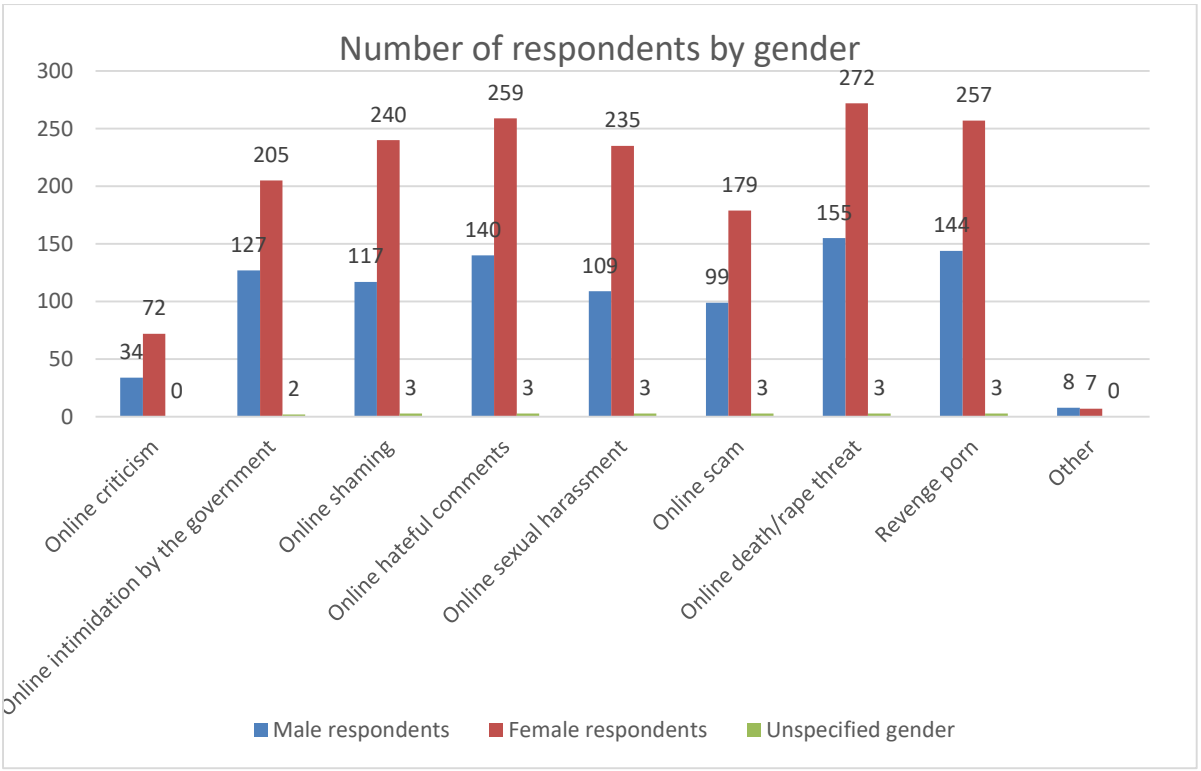
An online poster was created depicting the survivor as a supporter of adultery, sodomy, same-sex marriage and LGBT, with a comment, "Halal darahnya untuk dibunuh."

A fatal car accident occurred in May 2015 as result of an illegal race held by Familia Myvi Club (FMC) which involved six Myvis and a Pajero. The Myvi drivers were members of FMC of which the survivor was a spokesperson of. Although the survivor was not involved in the accident, he/she defended the six FMC members. At least three Facebook hate pages were created and at least a dozen comments on Facebook asking him/her to be hung, killed and beheaded - "Aku cari kau, Yana! Aku bunuh kau!"; "Bunuh je!;""Gantung je !";"…… Pancung kepala, terus senang…. ."

4.2 According to the Survey, 82.4 percent of respondents regarded online death and rape threats as online violence, this being the highest amongst all the other types of cyberharassment. This holds true for men and women across all age groups (save for women in their 40s).

Type of online activity	Male respondents (%)	Female respondents (%)
Online criticism	18.6	21.5
Online government intimidation	68.8	60.5
Online shaming	63.9	71.4
Online hateful comments	76.5	76.8
Online sexual harassment	59.5	69.9
Online scam	54.1	53.4
Online death/rape threat	84.6	81
Revenge porn	78.6	76.5
Other	4.3	2.1

What respondents consider as online violence (in percentage)



What respondents consider as online violence (in numbers)

4.3 Also, although a small fraction, those who spend time online have been recipients of death and/or rape threats.

4.4 In Malaysia, section 503 of the Penal Code and sections 211 and 233(1) of the CMA 1998 could be used to deal with online death and/or rape threats. In the latter, the provisions cover menacing communication that intends to threat or harass another person – for a discussion on the CMA 1998, please refer to Issue 1 above.

Section 503 of the Penal Code

4.5 Section 503 of the Penal Code deals with criminal intimidation – this is where a person "threatens another with any injury to his person, reputation or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat".

4.6 For this offence, one must prove two elements:

- There must be a threat with intent to cause one of the three outcomes; and
- Whilst there is no need to show that the outcomes actually occurred, there is a need to show that such threat was intentionally communicated to the person threatened by the accused.[100] In other words, the threat need not cause any effect upon the person threatened - all that is required is that it was made and communicated to the person threatened with the requisite intent. Also, the threat may be made to third parties and was intended that such threat be conveyed.[101]

4.7 The Penal Code does not provide definitions of the words "threaten" or "alarm". The ordinary dictionary meaning of the word "threaten" means "to intimidate by word or

[100] *Chandi Charan v Bhabataran* (1864) 2 Cr LJ 85.
[101] Annotated Statues of Malaysia, 2014, Issue 118, Vol. 5, at pg. 2502.

action". To "intimidate" means to "frighten, cow, usually in order to influence conduct". As regards the word "alarm", The Oxford Dictionary defines alarm as "to disturb, frighten, agitate".

4.8 In a Singapore case of *Ramanathan Yogendran v PP*,[102] the Court held that the threat must be sufficient to overcome the ordinary free will of a firm man. In this case, there had been a threat to kill and there was some objectively reasonable basis for the complainant to be alarmed; there was no indication that the appellant's threat was merely empty talk.

4.9 Although the reported cases under section 503 of the Penal Code do not relate to online harassment, a sample of the types of cases prosecuted under this section relate to pointing a gun at a person;[103] attacking someone with a *parang*;[104] threatening to stab victim with knife;[105] and acting under coercion and was forced by the plaintiff's director and shareholder to sign the written guarantee.[106]

Other jurisdictions

Ireland

4.10 The laws in Ireland regarding death threats and rape threats online are more expansive as it includes hate speech. Section 2(1) of the Prohibition of Incitement to Hatred Act 1989 makes it an offence for a person to publish or distribute written material; or use words, behave or display written materials, in a public place or if in a private place, the words, behaviour or material are heard or seen by persons outside the private place; or distribute, show or play a recording of visual images or sounds, that are threatening, abusive or insulting and are intended or likely to stir up hatred. "Hatred" in section 1 of the 1989 Act is defined as "hatred against a group of persons in the State or elsewhere on account of their race, colour, nationality, religion, ethnic or national origins, membership of the travelling community or sexual orientation".

4.11 In 2011, a case was prosecuted under section 2 of the 1989 Act – this case concerned the accused who created a Facebook page directed at Travellers[107] in 2009. The said Facebook page wrote in the 'information/description' of the page "Instead of using animals for shark bait, they could use knack babys [sic]. Also as food at feeding time in the zoo. And for testing new drugs and viruses".[108] The accused sent the page to three of his friends and the page and 644 members.

United Kingdom

4.12 In the UK, a number of provisions in the Public Order Act 1986 have been used to tackle online threats. Section 4 of the 1986 Act makes it an offence for a person to use, towards another person, threatening, abusive, or insulting words or behaviour, or distributes or displays any writing, sign or other visible representation that is threatening, abusive or insulting, with the intent to cause that person to believe that immediate unlawful violence will be used against him or another person, or to provoke the immediate use of unlawful violence by that person or another, or whereby that person is likely to believe that such violence will be used or it is likely that such violence will be provoked. The punishment

[102] [1995] 2 SLR 563; see also *Ameer Akhbar v Abdul Hamid,* [1997] 1 SLR 113.
[103] *Arsah Madi v. PP*, [2015] 1 LNS 1190.
[104] *PP v Hydhir Azni Che Yan*, [2011] 5 LNS 24.
[105] *Zainuddin Mahmud* v. PP, [2010] 2 CLJ 512.
[106] *Nuri Asia Sdn Bhd V. Fosis Corporation Sdn Bhd,* [2006] 5 CLJ 307.
[107] The Irish Traveller Movement is a national membership organisation representing Travellers and Traveller organisations founded in 1990. One of its core principles and objectives is to challenge the racism that Travellers face in Ireland, promoting integration and equality within Irish society.
[108] Irish Traveller Movement ICCPR Seanad Submission, <https://www.oireachtas.ie/.../Irish-Traveller-Movement-ICCPR-Seanad- Submission.docx> accessed 10 October 2016.

for this offence is (on summary conviction), imprisonment for a term not exceeding six months or a fine not exceeding level 5 on a standard scale or both.

4.13 In the case of *R v Stacey*,[109] the accused, when he was watching the rugby match between Wales and France and he saw rugby player Fabrice Muamba lying prostrate on the pitch, he posted a tweet on Twitter, "LOL fuck Muamba he's dead." As well as posting this message on his own account the Appellant linked the message to a site call Ha Ha, which meant that what he had written was capable of being read not just by those persons who followed the Appellant's Twitter account but by any other user of Twitter. The Appellant's message provoked very strong responses and the appellant responded to an African descent man's tweet, "I am not your friend, you wog cunt, go pick some cotton." Over the course of the next hour or thereabouts he posted at least eight messages which were extremely abusive and insulting. All the messages were available to be read by persons who could access Twitter. Two of these messages were expressly racial and couched in terms which can only be regarded as extremely offensive. They read, "You are a silly cunt your mother's a wog and your dad is a rapist, bonjour you scruff northern cunt;" and "Go suck a nigger dick you fucking aids-ridden cunt." The accused was convicted under section 4(1)(a) of the Public Order Act 1986 and sentenced to 56 days imprisonment.

4.14 Other relevant sections of the Public Order Act 1986 include:

- Section 4A – it is an offence for a person, who with the intent to cause a person harassment, alarm or distress, uses (a)uses threatening, abusive or insulting words or behaviour, or disorderly behaviour; or (b)displays any writing, sign or other visible representation which is threatening, abusive or insulting, causing that or another person harassment, alarm or distress. The punishment for this offence is (on summary conviction) imprisonment for a term not exceeding six months or a fine not exceeding level 5 on a standard scale or both.
- Section 5 of the same Act makes it an offence for a person if he/she (a)uses threatening or abusive words or behaviour, or disorderly behaviour; or (b)displays any writing, sign or other visible representation which is threatening or abusive, within the hearing or sight of a person likely to be caused harassment, alarm or distress. The punishment for this offence (on summary conviction) is a fine not exceeding level 3 on the standard scale.

4.15 Similar to Ireland, the UK has promulgated specific provisions to tackle racial hatred - sections 18 to 22 of the Public Order Act 1986 makes it an offence for a person to use threatening, abusive or insulting words or behaviour; or displays any written material which is threatening, abusive or insulting; or publishes any written material which is threatening, abusive or insulting; or presents or directs a public performance of a play is given which involves the use of threatening, abusive or insulting words or behaviour; or distributes, or shows or plays, a recording of visual images or sounds which are threatening, abusive or insulting; or provides, produces, directs or uses offending words or behaviour in programme involving threatening, abusive or insulting visual images or sounds:

- With the intention to stir up racial hatred; or
- having regard to all the circumstances racial hatred is likely to be stirred up

4.16 As for hatred against persons on religious grounds or grounds of sexual orientation, sections 29B to 29F makes it an offence for any person to use threatening words or behaviour, or displays any written material which is threatening; or publishes or distributes written material which is threatening; or presents or directs public

[109] Appeal No: A20120033, Swansea Crown Court, 30 March 2012, <https://www.judiciary.gov.uk/wp-content/uploads/JCO/Documents/Judgments/appeal-judgment-r-v-stacey.pdf> accessed 4 February 2017.

performance of a play is given which involves the use of threatening words or behaviour; or distributes, or shows or plays, a recording of visual images or sounds which are threatening; or provides, directs or produce a programme involving threatening visual images or sounds is included in a programme service:

- if he/she intends thereby to stir up religious hatred or hatred on the grounds of sexual orientation.

Hong Kong

4.17 In Hong Kong, a number of provisions address threats made online, including threatening a person to do an unlawful sexual act and blackmail. The first is section 24 of the Crimes Ordinance (Cap. 200), which is similar to section 503 of the Malaysian Penal Code. Section 24 makes it an offence for a person to threaten another person with injury to their person, reputation or property, or with any illegal act with intent to alarm the person so threatened or to cause that person to do something they are not legally bound to do, or to cause them not to do something they are legally entitled to do. This offence is punishable upon summary conviction by a fine of $2,000 and two years' imprisonment, and upon indictment by imprisonment for five years.

4.18 Section 119 of the Crimes Ordinance makes it an offence for a person to procure another person by threats or intimidation to do an unlawful sexual act[110] in Hong Kong or elsewhere. Procurement by threats is punishable by imprisonment for 14 years.

4.19 In two cases brought under section 119, *HKSAR v Wong Dawa Norbu Ching Shan*[111] and *HKSAR v Liang Fu Ting,*[112] the facts of which are similar, the defendant threatened to post nude photographs of the victim on the Internet and social media platforms unless the victim engaged in unwanted sexual intercourse with the defendant. Both defendants were convicted, respectively – in the former case, the defendant was sentenced to two years and six months imprisonment and in the latter, the Court sentenced the defendant to 20 months imprisonment for each charge.

4.20 The Hong Kong authorities have also resorted to section 23 of the Theft Ordinance to deal with certain types of cyber harassment. Section 23 states that "a person commits blackmail if, with a view to gain for himself or another or with intent to cause loss to another, he makes any unwarranted demand with menaces; and for this purpose a demand with menaces is unwarranted unless the person making it does so in the belief - (a) that he has reasonable grounds for making the demand; and (b) that the use of the menaces is a proper means of reinforcing the demand.

4.21 In the case *HKSAR v Chai Mei Kwan*,[113] which resulted in 20 months' imprisonment with the defendant's plea of guilty, after having sexual intercourse with the victim, the defendant sent him SMS messages demanding money. In another SMS, she told him there was a video of their intimacies, which could be distributed to "everyone". In sentencing Deputy District Judge Joseph To remarked "There are two aggravating factors in this case. Firstly, the defendant did not just utter empty words; she had equipped herself with the video clip showing her and the victim in compromising circumstances. Secondly, the threatened means of dissemination via the computer must have filled the victim with alarm; it is common knowledge that the Internet knows no borders and once uploaded information is difficult to erase."

---

[110] According to section 117(1A) of the Crimes Ordinance, an unlawful sexual act is committed if, and only if, that other person: (a) has unlawful sexual intercourse; (b) commits buggery or an act of gross indecency with a person of the opposite sex with whom that person may not have lawful sexual intercourse; or (c) commits buggery or an act of gross indecency with a person of the same sex.

[111] [2013] HKDC 853; DCCC 70/2013 (10 June 2013).

[112] [2011] HKDC 1262; DCCC 535/2011 (31 August 2011).

[113] [2011] HKDC 1208; DCCC 412/2011 (11 August 2011).

4.22 Closely related to the offences of blackmail is section 60 of the Crimes Ordinance (Cap. 200), which makes it an offence for a person who without lawful excuse intentionally destroys or damages any property belonging to another person or is reckless as to whether any such property is destroyed or damaged is guilty of an offence.

4.23 In *HKSAR v Ko Kam Fai*,[114] the defendant hacked into the e-mail accounts of his two victims and changed some data in their computers. As a result of the large number of emails he sent them, their e-mail accounts were overloaded to the extent that they became inoperative. His actions amounted to criminal damage, as the computers ceased to operate as a result of his activities. Amongst the e-mails sent by the Applicant to X and Y was a message which read: "Don't you believe that I will go to your hall to rape you."

Australia

4.24 In Australia, most Australian states have specific offences of threatening to kill or cause serious harm. A typical provision is section 31 of the Crimes Act 1900 of New South Wales, which states that "a person who intentionally or recklessly, and knowing its contents, sends or delivers, or directly or indirectly causes to be received, any document threatening to kill or inflict bodily harm on any person is liable to imprisonment for 10 years".

4.25 For this offence, section 31(2) of the said Act states that it is immaterial "whether or not a document sent or delivered is actually received, and whether or not the threat contained in a document sent, delivered or received is actually communicated to the person concerned or to the recipient or intended recipient of the document (as relevant in the circumstances)".

4.26 Other threat offences include, threatening to cause bodily harm (section 31); grievous bodily harm (section 31); to destroy or damage property (section 199); to do any injury, or cause any detriment (Criminal Code 1983 (NT) section 200; Criminal Code 1899 (Qld) section 359); detriment on any kind (Criminal Code 1913 (WA) sections 338(d), 338B); to inflict serious injury (Crimes Act 1958 (Vic) section 21); to cause 'harm to the person or property of another (Criminal Law Consolidation Act (SA) section 19(2)); and to injure, endanger or harm (Criminal Code 1913 (WA) sections 338(a), 338B).[115]

4.27 In the case of *Usmanov v R,*[116] Usmanov uploaded six nude photographs of his ex-girlfriend to Facebook without her permission. After she asked that he take them down he did so, but he then reposted them and sent them to her roommate. Upon prosecution, Usmanov pleaded guilty to an offence of publishing an indecent article under s 578C of the Crimes Act 1900.[117] In imposing a six month imprisonment, the Magistrate took into consideration that he (Usmanov) failed to take them (the photos) off completely and that it was not clear how many people had access to the Facebook page and, therefore, how broad the distribution of the material was. The Magistrate felt that there was a need for deterrence for these sorts of offences because they are offences that are easy to commit and can have a significant impact so far as the victim is concerned.

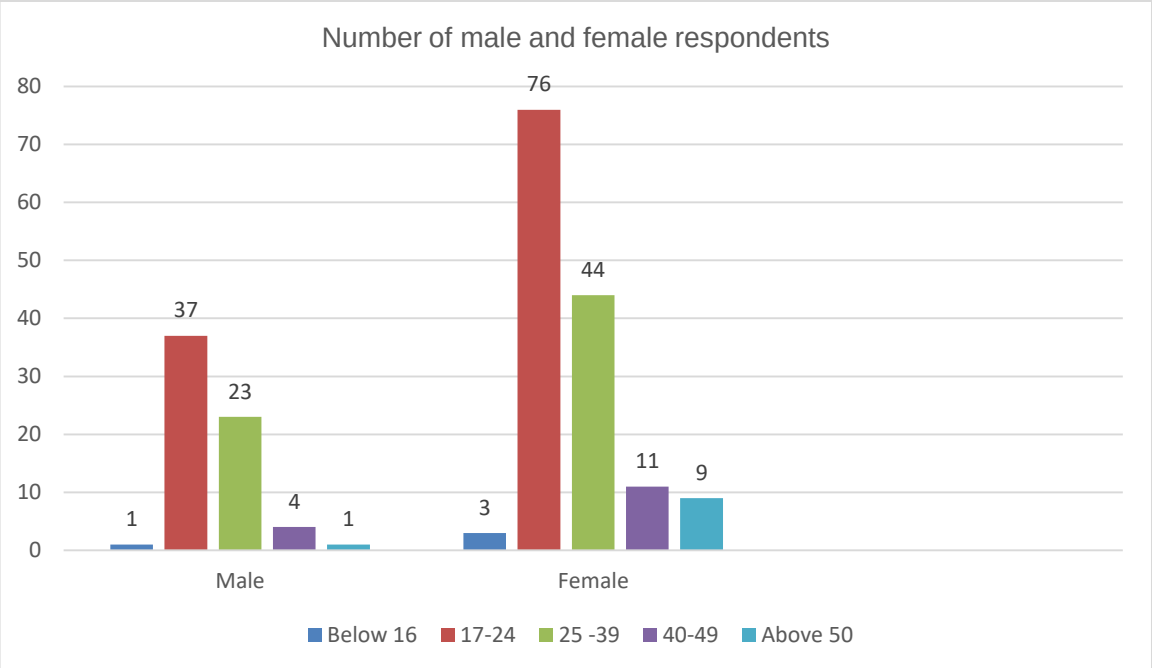
Analysis

[114] [2001] HKCA 221; [2001] 3 HKC 181; CACC 83/2001 (20 June 2001).
[115] Kift, Sally; Campbell, Marilyn; Butler, Des, @Cyberbullying in Social Networking Sites and Blogs: Legal Issues for Young People and Schools" [2010] *JlLawInfoSci 13*; (2010) 20(2) *Journal of Law, Information and Science* 60, <http://www.austlii.edu.au/au/journals/JlLawInfoSci/2010/13.html#fn93> accessed 8 November 2016.
[116] [2012] NSWDC 290 (15 February 2012).
[117] 'Cyberbullying in Australia (3 May 2013), <https://cybercrime2013.wordpress.com/2013/05/03/australian-cases/> accessed 8 November 2016.

4.28 The laws in this area can be divided into two categories – firstly, in some jurisdictions like Ireland and the UK, authorities have tried to use provisions that specifically tackle threats, abusive or insulting communication that is intended to stir up hatred against a person or groups of person based on their race, religion, sexual orientation or other grounds, to deal with abusive comments made online. Although, in Ireland, the Irish Traveller Movement case was criticised by some as it was observed that the prosecution failed because of the inadequacy of section 2(1) of the Prohibition of Incitement to Hatred Act 1989 to criminalise hate speech.[118]

4.29 Secondly, the authorities in Ireland, UK, Hong Kong, and Australia have also resorted to criminal intimidation laws where it is a crime to threaten to injure another person or to blackmail a person from doing or forbidding the other person from carrying out a particular act. For these offences, it is not necessary to show that the outcome actually occurred where the offence is proven once it was communicated to that person.

4.30 It would appear that section 503 of the Penal Code could be applied to threats of rape or death received online as it is immaterial that the threat did not cause the victim/survivor to be alarmed. There are instances where recipients of death threats or rape threats were not alarmed and they were able to ignore the comments received because "it was not affecting their lives" or "they would fight back in a civilised way". According to the Survey conducted, when asked whether they felt fearful, threatened or uneasy because of comments of responses received, 57.3 percent answered 'no'. Those who felt fearful, threatened or uneasy (42.7 percent) are as follows:



Disaggregated data showing the percentage of female and male respondents by age group who have felt fearful, threatened or uneasy online

4.31 A similar result was observed for the survey conducted with the LGBTQI community where majority (59.7 percent) did not feel threatened or fearful and only 35.8 percent felt frightened.

4.32 However, one element that must be proven for section 503 of the Penal Code is the need to show that the threat was communicated to the victim/survivor. This could be

[118] Irish Traveller Movement ICCPR Seanad Submission, <https://www.oireachtas.ie/.../Irish-Traveller-Movement-ICCPR-Seanad- Submission.docx> accessed 10 October 2016.

problematic as there are some instances where the alleged offender makes threatens the victim/survivor in an indirect manner. For example, the alleged offender makes a threat using his or her Twitter account without tagging the victim/survivor or the alleged offender sets up a hate page on Facebook about the victim/survivor without necessarily communicating the threats directly to the victim/survivor. Because of the rapidity and anonymity that social media platforms such as Twitter and Facebook offers, in these cases, the situation could still escalate quickly affecting the personal safety of victims/survivors. Whether an offence under section 503 could still be proven in this instance, remains to be seen.

4(a) Are section 503 of the Penal Code and/or sections 211 and/or 233(1) of the CMA 1998 sufficient to deal with the problem of death threats, rape threats and other abusive communication made online?

ISSUE 5: WHETHER THE CURRENT LAW IS SUFFICIENT TO DEAL WITH THE OFFENCE OF USING CYBER TECHNOLOGY TO SERIOUSLY INTERFERE WITH ANOTHER'S PRIVACY

5.1 Apart from harassing behaviour, which in most jurisdictions (such as UK, Australia, and Ireland) require persistent behaviour (see above in Issue 1), it is observed that there are times when uploading a single posting could seriously interfere with the privacy of the survivor/victim.[119] The Survey showed that 13.8 percent of respondents have had their personal details or photographs revealed online without their consent (see above).

5.2 Also, the PeopleACT collated incidents where the alleged offender would post on one or several social media platforms, a copy of the identification card or the birth certificate of the survivor/victim or personal details such as home address, date of birth, or car registration number. Incidents of breach of private information include:

A group of hackers hacked into the survivor's email account and posted a PowerPoint presentation containing his/her private information such as his/her identification number and voting details on a website, linking the survivor to Makcik Hajjah Sitt Al-Wuzara (an online profile allegedly notorious for making anti-Islamic sentiments online). As result, the survivor received multiple death and rape threats and hateful comments from random people via his/her phone, Facebook and website between August to October/November 2011.

In 2014, a survivor posted his/her opinion on the "Allah-Herald" case on Facebook. Apart from threats, the survivor's private information such as car registration and identity card number were shared online.

[119] Issues Paper on Cyber-crime affecting personal safety, privacy and reputation including cyber-bullying' (LRC IP 6-2014, *Law Reform Commission*, <http://www.lawreform.ie/_fileupload/Issues%20Papers/ip6Cybercrime.pdf> accessed 24 March 2016.

The survivor started an online petition calling for the removal of the Prime Minister's portrait from his/her university. Subsequently, a person posted on Facebook urging the public to submit private information about the survivor's family members to that person - "Sesiapa yang tahu mengenai keluarga pelajar ini juga boleh beri maklumat kepada saya. Kita mahu melihat sesuci mana pula keluarganya yang mampu menghantar anak ke luar negara ini." Subsequently, more blog posts about the survivor emerged, mainly containing the survivor's family members' full names, identification card numbers, and home address. The survivor then deactivated his/her Facebook account for a few weeks and reactivated with stronger privacy setting.

A fatal car accident occurred in May 2015 as result of an illegal race held by Familia Myvi Club (FMC) which involved six Myvis and a Pajero. The Myvi drivers were members of FMC of which the survivor was a spokesperson of. Although the survivor was not involved in the accident, he/she defended the six FMC members. Some went as far as to dig up private information (identification number, car registration number, phone number, etc.) and photos of the survivor, and posted those details online.

In 2014, a survivor met an accident with an elderly man and he/she verbally abuse the man and used a steering lock to hit the hood of his car repeatedly. The incident was recorded by an onlooker and uploaded onto YouTube and Facebook. The survivor's car registration number was shared online and the survivor was threatened with violence: - "(Hashtag survivor's car plate number), you really in deep shit. People are hunting you down on the highway. Get off the highway and burn your car, bitch. LOL;" "Boleh pulak terserempak! Haha! Rezeki aku. (Hashtag survivor's car plate number) God bless! Area Cyberjaya;" "Alaaa…lajunya bawak. Baru nak mintak autograf kat bumper. (Hashtag survivor's car plate number)";"Share info on (description of survivor's car) – name and shame! Share whatever info you have on her for bullying that uncle."

5.3 In such a situation, even if the relevant section in the CMA 1998 is amended to include persistent behaviour, the problem mentioned above would not be able to fulfil the persistent behaviour requirement, and yet such a communication could be damaging to the victim/survivor and could breach his/her right of privacy.[120] Once a communication is uploaded online, it remains online permanently and it has the potential to go viral; as such, any harm caused by the breach of privacy could have a long-term effect.[121]

5.4 In terms of the right to privacy, the relevant laws in Malaysia are the tort of invasion of privacy, the Personal Data Protection Act 2010, and to a certain extent, section 509 of the Penal Code.

Section 509 of the Penal Code

5.5 Briefly, section 509 makes it an offence for any person who intends to insult the modesty of any person "utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen by such person, or ***intrudes upon the privacy of such person***" (emphasis added). For a discussion on section 509, please see Issue 2 above.

Right to privacy

[120] Issues Paper on Cyber-crime affecting personal safety, privacy and reputation including cyber-bullying' (LRC IP 6-2014, *Law Reform Commission*, <http://www.lawreform.ie/_fileupload/Issues%20Papers/ip6Cybercrime.pdf> accessed 24 March 2016.

[121] Issues Paper on Cyber-crime affecting personal safety, privacy and reputation including cyber-bullying' (LRC IP 6-2014, *Law Reform Commission*, <http://www.lawreform.ie/_fileupload/Issues%20Papers/ip6Cybercrime.pdf> accessed 24 March 2016.

5.6 Malaysian case law regarding right to privacy appears to be unsettled. The argument of the actionable tort of privacy was argued in the case of *Ultra Dimension Sdn Bhd v Kook Wei Kuan*[122] where the appellant had taken a photograph of a group of kindergarten pupils at an open area outside the kindergarten, where the respondent was captured in the said photograph; the appellant did not obtain the consent of the parents/guardian of the respondent. The photograph was published by the appellant in two local newspapers with the theme "Bonus Link Share Your Points". The respondent claimed damages for invasion of privacy and breach of confidence. The High Court held that the publication of the photograph did not give the respondent a cause of action as the facts of the case did not fall within the boundaries of any recognised and existing tort (of defamation, infringement of copyright, or nuisance). The High Court went further to state that a cause of action may only arise if the photographs were "highly offensive in nature and showed a person in an embarrassing position or pose". As for the claim for breach of confidentiality, the High Court held that the photograph was not a piece of confidential information as the appellant is the maker of the said photograph and not the respondent. There can only be a breach of confidence if the information is confidential in nature; secondly, there was no contract between the appellant the respondent; thirdly, the photograph was taken at a public place i.e., an open area outside a kindergarten which is open to the public. Therefore, any passerby which is in the area is free and is at liberty to take photographs in that area; lastly, there was no photographer-customer relationship between the appellant and the respondent and thus there was no understanding between both parties regarding the usage of the said photograph.

5.7 However, the Court of Appeal took a rather different position on the right to privacy in the case of *Maslinda binti Ishak v Mohd Tahir bin Osman & 3 Ors*[123](for the facts of this case see above in Issue 3). The Court of Appeal held that there was abundance of evidence as regards the invasion of privacy of the appellant. Subsequently, in *Sivarasa Rasiah v Badan Peguam Malaysia*, the Federal Court, in construing the ambit of article 5(1) of the Federal Constitution, which guarantees the right to personal liberty, held that "it is patently clear from a review of the authorities that "personal liberty" in article 5(1) includes within its compass other rights such as the right to privacy".

5.8 This approach towards recognising the tort of right to privacy continued in *Lee Ewe Poh v Dr. Lim Teik Man & Anor.*[124] The plaintiff was suffering from haemorrhoids and consulted the first defendant who was a General and Colorectal Surgeon practising in Loh Guan Lye Specialist Centre owned and operated by the second defendant. The plaintiff was admitted to the said Specialist Centre to remove her haemorrhoids. She later discovered that the first defendant had taken photographs of her anus during the procedure. She claimed a violation of her right to privacy and dignity by the first defendant as she was never asked nor did she give her consent to the first defendant to photograph her private part when under anaesthesia. The first defendant claimed that this was in accordance with accepted medical practice – one photograph to be taken before the procedure and one after the procedure; this was to facilitate easy explanation to the patient after the procedure. There was no publication of the plaintiff's identity and the photographs were intended for the plaintiff's medical records. Referring to the Court of Appeal decision in *Maslinda Ishak,* the High Court held that the right to privacy is an actionable right – the "privacy of a female in relation to her modesty, decency, and dignity in the context of the high moral value existing in our society is her fundamental right in sustaining that high morality that is demanded of her and it ought to be entrenched". The Court further held that in order for a surgeon to take photographs of a female patient's

[122] [2004] 5 CLJ 285.
[123] [2009] 1 LNS 891.
[124] [2011] 4 CLJ 397.

intimate parts of her anatomy as in this case, the proper procedure to adopt is to obtain her prior consent whether it is written or oral.

5.9 In *Lew Cher Phow @ Lew Cha Paw & Ors v Pua Yong Yong & Anor,*[125] on 13 May 2006, the defendants installed five closed-circuit televisions (CCTV) cameras in their house; four of the cameras were installed at the front porch and one was installed at the rear of the house. Of these five CCTV cameras, only one camera (Camera No. 3) was pointing directly at the plaintiff's house. Camera No. 3 was attached to a nine feet pole which is about 16 feet from the chain-link fence. The plaintiffs complained that Camera No. 3 was directed and focused at and monitoring and capturing images of the plaintiffs' front courtyard and the camera at the rear of the house was directed and focused at and monitoring and capturing images of the rear portion of the plaintiffs' house. The plaintiffs' felt that they were being spied on and their right to privacy has been infringed. On the issue of right to privacy, the High Court held that the defendants' continuing act of putting the plaintiffs' under overt surveillance represents a failure of respect of the plaintiffs' dignity and autonomy. It constitutes an intrusive surveillance on the plaintiffs' private and family life and home. The defendants' fear for their safety and security do not justify their actions and cannot override the plaintiffs'' right to privacy. The said Court held that everyone has a right to be free from continuous video surveillance in his own property. The Court took cognisance of article 14 of the UDHR, article 17 of the ICCPR and article 8 of the ECHR. The Court held that the views in *Ultra Dimension* were not keeping with times and that the cases of *Maslinda Ishak, Lee Ewe Poh* and *Sivarasa Rasiah* indicated that the Malaysian courts are in favour of recognising the right to privacy. It consequently recognised the right to privacy as a fundamental right which is entitled to protection. On the facts of the case, the High Court held that the plaintiffs' right to privacy has been violated and ordered the defendants to dismantle and remove Camera No.3 and granted an injunction to restrain the defendants from installing any CCTV camera which points into or which is directed at the plaintiffs' house.

5.10 However, the scope of the right to privacy was somewhat narrowed in the case of *M.Mohandas Gandhi & Anor v Ambank (M) Berhad & Anor*[126] - although the High Court followed the decisions in *Maslinda Ishak* and *Lee Ewe Poh* recognising that invasion of privacy is a cause of action, it however held that this right is limited to matters of private morality and modesty only. Based on the facts of this case, the High Court held that there was no invasion of the plaintiff's privacy as the information (the information relate to legal proceedings filed against the plaintiff, which was stored in the second defendant's database) is a matter of public record and is in the public domain.

5.11 Similarly, the Courts departed from the decisions in *Maslinda Ishak* and *Lee Ewe Poh* – in *John Dadit v Bong Meng Chat & 4 Ors*,[127] the Court held that there is no written law in force in Malaysia for such right to privacy or tort of invasion of privacy. It held that the decision of the Courts in the *Maslinda Ishak* and *Lee Ewe Poh* were not the *ratio decidendi* of the judgement and hence not binding. Also, in *Mohamad Izaham Mohamed Yatim v Norina Zainol Abidin & Ors*,[128] (see above for the facts of the case) the High Court held that invasion of privacy was not an actionable tort in Malaysia. The Court went on to state that even if it accepts and follows the decisions in *M. Mohandas Gandhi* and *Lee Ewe Poh*, where the tort of invasion of privacy is limited to matters of private morality and modesty, the Court does not find that such an action has been disclosed in this case.

[125] [2011] 1 LNS 1528.
[126] [2014] 1 LNS 1025.
[127] [2015] 1 LNS 1465.
[128] [2015] 7 CLJ 805.

5.12 There are no reported cases of interference of the right to privacy relating to cyberharassment.

Personal Data Protection Act 2010

5.13 Apart from the actionable tort of privacy, the Personal Data Protection Act 2010 (PDPA 2010) could be used to protect personal data, including sensitive data.

5.14 The 2010 Act defines "personal data" as any information in respect of commercial transactions, which is being processed by means of equipment operating automatically in response to instructions given; or recorded with the intention of being processed or recorded as part of a relevant filing system. The data in question must relate directly or indirectly to a data subject who is identified/identifiable from that information, including any sensitive personal data and expression of opinion about the data subject. However, it excludes information processed for credit reporting business.

5.15 The PDPA 2010 applies to any person who processes; and who has control over or authorises the processing of any personal data in respect of commercial transactions. It is based on seven Personal Data Protection Principles:

- **General Principle** – the General Principle requires that personal data other than sensitive personal data[129] should not be processed unless the data subject has consented. Sensitive personal data can only be processed if there is explicit consent[130] by the data subject and the processing is necessary for the stated reasons in section 40(1)(b) of the 2010 Act; for example for the purposes of exercising or performing any right or obligation, to protect the vital interests of the data subject or another person for medical purposes, or for the administration of justice;
- **Notice and Choice Principle** – this requires the data user to inform (by written notice) the data subject of how the data subject's personal data will be processed – for example, description of the personal data, purposes for which it is collected or further processed, source of the personal data, or, class of third parties to whom the data user discloses;
- **Disclosure Principle** – this restricts the data user from disclosing, without the consent of the data subject, for any purpose other than the purpose that was disclosed at the time of collection of the personal data;
- **Security Principle** – this requires the data user to take all practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction. The Personal Data Protection Standards 2015 prescribe certain security measures to taken in order to comply with this principle;
- **Retention Principle** – this principle limits the period that the data user may keep personal data of data subjects, i.e., not longer than necessary for the fulfilment of the purpose for which it is processed. The data user bears the responsibility to ensure that personal data is destroyed or permanently deleted if it is no longer required for the said purpose;
- **Data Integrity Principle** – this obliges the data user to take reasonable steps to ensure that the personal data is accurate, complete, not misleading, and kept up-to-date by having regard to the purpose it was collected;

[129] Section 4 of the 2010 Act states that "sensitive personal data" means "any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data as the Minister may determine or by order published in the Gazette".

[130] Explicit consent is not defined in the 2010 Act but in Opinion 15/2011 of the European Commission's Data Protection Working Party, this means individuals are given a proposal to agree or disagree with a particular use or disclosure of their personal information and they respond actively to the question, orally or in writing.

- **Access Principle** – this gives the data subject the right to access his/her personal data and correct that personal data where the personal data is inaccurate, incomplete, misleading, or not up-to-date.

Other jurisdictions

Ireland

5.16 In Ireland, interestingly, section 98 of the Postal and Telecommunications Services Act 1983 was used to deal with an intrusion of privacy of posting private communications online. Section 98 prohibits the interception of telecommunication messages without authority. In the case of *Herrity v Associated Newspapers (Ireland) Ltd,*[131] the plaintiff, a married woman was having an extra-marital affair with a priest and the details of which was published by the defendants (the newspaper); details were supplied to the defendant by the plaintiff's husband who had hired a private investigator who had tapped her telephone and recorded her conversations with the priest. The transcripts were published by the defendant. The plaintiff sued the defendants claiming that the publication of the transcripts amounted to a breach of her right to privacy and that the defendant could not claim that their actions were lawful in circumstances where the material published was obtained as a result of the commission of a serious criminal offence.

5.17 The High Court held that the publication of the telephone transcripts was obtained in breach of section 98 of the Postal and Telecommunications Services Act 1983. The defendant cannot assert the right to freedom of expression to publish telephone conversations where the legislature has expressly prohibited the interception of telecommunications messages. The Court explained that the purpose of section 98 is to protect the privacy of telephone conversations and this is an exception to the right to freedom of expression. As regards the defendant's argument of public interest i.e. that the Catholic priest is a public figure and the conduct of the priest may be subject to public scrutiny, the Court rejected this argument and held that having regard to the means the information was obtained (in breach of section 98) and the type of disclosure that occurred, public interest remains subject to the right of privacy.

5.18 Ireland also has a similar law to Malaysia regarding data protection. Passed in 1998, section 4(1) of the Data Protection Act 1998 makes it an offence for a data controller[132] to disclose any personal data; personal data is defined as "data relating to a living individual who can be identified either from the data or from the data in conjunction with other information in the possession of the data controller" and this includes images, videos, comments about the person and other identifying information such as phone number or address[133].

5.19 The term "data controller" was interpreted by the EU Working Party on the Protection, to include social networking and other websites.[134]

European Union

---

[131] [2009] 1 IR 316.

[132] Section 1 off the Data Protection Act 1988 defines a "data controller" as "a person who, either alone or with others, controls the contents and use of personal data".

[133] Law Reform Commission, 'Issues Paper on Cyber-crime affecting person safety, privacy and reputation including cyber-bullying (LRC IP 6-2014), <http://www.lawreform.ie/_fileupload/Issues%20Papers/ip6Cybercrime.pdf> accessed 20 April 2016.

[134] Article 29 Data Protection Working Party Opinion 5/2009 on online social networking 01189/09/EN WP 163 (June 2009) in Law Reform Commission, 'Issues Paper on Cyber-crime affecting person safety, privacy and reputation including cyber-bullying (LRC IP 6-2014), <http://www.lawreform.ie/_fileupload/Issues%20Papers/ip6Cybercrime.pdf> accessed 20 April 2016.

5.20 Generally, EU Directive 95/46/EC[135] relates to the protection of individuals with regard to the processing of personal data and on the free movement of such data.[136] Article 2 defines "personal data" as "any information relating to an identified or identifiable natural person" and "processing of personal data shall mean operation(s) which is performed upon personal data, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction"

5.21 Similar to the PDPA 2010, article 7 of the said Directive states that "Member States shall provide that personal data may be processed only if a) the data subject has given consent, b) the processing is necessary for the performance of a contract, c) processing is necessary for compliance with a legal obligation to which the controller is subject, d) processing is necessary in order to protect the vital interests of the data subject, e) processing is necessary for the performance of a task carried out in the public interest".

5.22 The EU Data Protection Working Party[137] issued an opinion that the household exemption (an individual who processes personal data "in the course of a purely personal or household activity") does not apply to an social network service (SNS)[138] user "who acts on behalf of a company or association or uses social media as a platform to advance commercial, political or charitable goals"; or any individual who posts personal data of another person without the other person's consent – in both instances, the user assumes the full responsibilities of a data controller and consent of persons concerned would be required.[139]

5.23 The said Working Party felt that profile data, postings and stories contributed by a user is limited to self-selected contacts and when an individual posts such personal data to a high number of third party contact, the high number of contacts could be an indication that the exception does not apply and the user would be considered a data controller.[140] Therefore, an individual who posts personal information about another person on a public website or a social networking platform that is accessible by a large number of

[135] There is a proposal for a new regulation (COM (2011) 12) to replace Directive 95/46/EC, but there are no changes relating to the Articles related to cyber harassment European Union; see further 'Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)', 25th January 2012, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN> accessed 20 October 2016.

[136] European Union, Directive 95/46EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. 24th October1995, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN> accessed 16 October 2016.

[137] The Article 29 Working Party, composed of representatives from all EU Data Protection Authorities, the EDPS and the European Commission, was set up under the Directive 95/46/EC. It has advisory status and acts independently. <http://ec.europa.eu/justice/data-protection/> accessed 30 March 2017.

[138] SNS can broadly be defined as online communication platforms which enable individuals to join or create networks of like-minded users. In the legal sense, social networks are information society services, as defined in Article 1 paragraph 2 of Directive 98/34/EC as amended by Directive 98/48/EC. SNS share certain characteristics: - users are invited to provide personal data for the purpose of generating a description of themselves or 'profile'; SNS also provide tools which allow users to post their own material (user-generated content such as a photograph or a diary entry, music or video clip or links to other sites; 'social networking' is enabled using tools which provide a list of contacts for each user, and with which users can interact, Opinion 5/2009 on online social networking, 01189/09/EN WP 163, Article 29 Data Protection Working Party, <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf> accessed 30 March 2016.

[139] Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking 01189/09/EN WP 163 (June 2009) in Law Reform Commission, 'Issues Paper on Cyber-crime affecting person safety, privacy and reputation including cyber-bullying (LRC IP 6-2014), <http://www.lawreform.ie/_fileupload/Issues%20Papers/ip6Cybercrime.pdf> accessed 10 October 2016.

[140] Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking 01189/09/EN WP 163 (June 2009) in Law Reform Commission, 'Issues Paper on Cyber-crime affecting person safety, privacy and reputation including cyber-bullying (LRC IP 6-2014), <http://www.lawreform.ie/_fileupload/Issues%20Papers/ip6Cybercrime.pdf> accessed 10 October 2016.

people would be considered a data controller within the meaning of section 1 of the 1998 Act and any disclosure would require prior consent of other persons.[141]

5.24 In the *Lindqvist* case,[142] the Court of Justice of the European Union (ECJ) dealt with a breach of Directive 95/46. Mrs. Lindqvist, a church worker, put personal data about her fellow church volunteers on a website. Mrs. Lindqvist was fined 4000SK by a Swedish Court, which she felt was disproportionate. The ECJ held that "the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data wholly or partly by automatic means within the meaning of Article 3(1) of Directive 95/46".

Hong Kong

5.25 In Hong Kong, section 4 of the Personal Data (Privacy) Ordinance requires a data user[143] to abide by the data protection principles set out in Schedule 1 of the Ordinance. Similar to the PDPA 2010, Principle 1 requires that personal data must be collected for a lawful purpose and fair way, for a purpose directly related to a function /activity of the data user. Data subjects must be notified of the purpose and the classes of persons to whom the data may be transferred. Data collected should be necessary but not excessive.[144] As such, the collection of personal data for criminal intimidation is not for a lawful purpose.[145]

5.26 Section 64 of the Ordinance makes it an offence for a person to disclose any person data of a data subject, which was obtained from a data user without the latter's consent and with an intent to i) obtain gain for himself/herself or another person; or ii) cause loss to the data subject or if the unauthorised disclosure causes psychological harm to the data subject.[146] The penalty for the offences is a fine of HK1 million and imprisonment for five years.

5.27 According to the Office of the Privacy Commissioner for Personal Data, it does not matter that the personal data has been published elsewhere or is publicly available. For example, if a person downloads intimate photos of a known individual from a public website and if that person knew the photos were leaked as a result of a data breach by a data user, and sells the photos for profit, this would be in contravention of Principle 3 of the Personal Data (Privacy) Ordinance.

5.28 The Privacy Commissioner for Personal Data has stated that there is a reasonable expectation of personal data privacy required by Principle 3.[147] The test is whether a reasonable person in the data subject's situation would find the reuse of the data unexpected, inappropriate or objectionably, taking into account the sensitivity of the personal data; the realistic risks of harm (identity theft, financial loss, harassment, injury to feelings) – for example the unrestricted disclosure of the name and residential address of the data subject online will expose the data subject to risks of his or her personal safety such as stalking and surveillance; the commercial use of the personal

---

[141] Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking 01189/09/EN WP 163 (June 2009) in Law Reform Commission, 'Issues Paper on Cyber-crime affecting person safety, privacy and reputation including cyber-bullying (LRC IP 6-2014), <http://www.lawreform.ie/_fileupload/Issues%20Papers/ip6Cybercrime.pdf> accessed 20 April 2016.

[142] ECJ C-101/01, (6 November 2003).

[143] Section 2 of the Ordinance defines "data user" as a "person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data".

[144] <https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html> accessed 19 October 2016.

[145] <www.pcpd.org.hk/english/publications/files/GN_public_domain_e.pdf> accessed 19 October 2016.

[146] <www.pcpd.org.hk/english/publications/files/GN_public_domain_e.pdf> accessed 19 October 2016.

[147] <www.pcpd.org.hk/english/publications/files/GN_public_domain_e.pdf> accessed 19 October 2016.

data that do not serve the interest of the data subject; and the combining, re-arranging and/ or matching of personal data from different public sources for profiling which result in function creep[148] and inaccurate inferences being made against the data subject.[149]

Analysis

5.29 Firstly, although Section 509 of the Penal Code includes an element of intrusion of a person's privacy, it captures only a very narrow form of cyberharassment, i.e. an incident where the post or comment is intended to insult the modesty of a person. Therefore, arguably, it would be quite difficult to bring a prosecution under section 509 for an incident where the alleged offender uploads merely intimate/personal details of the victim/survivor, for example, the identification card or the residential address of the victim/survivor.

5.30 As regards the PDPA 2010, the protection it affords applies only if the communication falls within the definition of personal data i.e. information in respect of ***commercial transactions*** (emphasis added) and the data must relate directly or indirectly to the data subject who is identified/identifiable form the information. In this regard, "commercial transactions" means "any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance, but does not include a credit reporting business carried out by a credit reporting agency under the Credit Reporting Agencies Act 2010".

5.31 Because of the limitation to commercial transaction, it will exclude many cyber harassment incidents where personal details posted by alleged offenders, on social media platforms, having nothing to do with the supply or exchange of goods or services, agency, investments, financing, banking, or insurance.

5.32 And unlike the EU Directive 95/46/EC where it has been stated that individuals posting personal data on a public website about another person without his or her consent would be treated as a data controller and would have to abide by the obligations set out in EU Directive 95/46/EC, the PDPA 2010 does not adopt a similar approach. As such, it would be difficult for a victim/survivor of cyberharassment to avail himself or herself to the protection afforded by the PDPA 2010.

5.33 As to the actionable tort of invasion of privacy, as mentioned earlier, the law in this area remains unsettled and it would appear that the Courts are still contending with the idea of whether to recognise the right to privacy as a fundamental liberty (as recognised in *Maslinda Ishak, Lee Ewe Poh, and Sivarasa Rasiah*), or whether the right to privacy is limited to matters of private morality and modesty only (*M. Mohandas Gandhi*), or whether there is no tort of invasion of privacy (*John Dadit* and *Mohamad Izaham Mohamad Yatim*). As such, although a victim/survivor of cyberharassment could arguably avail themselves to this tort, it must be acknowledged that this may be a challenging task.

5.34 As the tort of invasion of privacy and the PDPA 2010 offers remedies only in very narrow circumstances, the question to be contemplated is whether the action of revealing personal details or intimate actions (that do not amount to outraging modesty) in a one-off action and using cyber enabled technology, amounts to serious interference with a person's right to privacy.[150]

---

[148] Function creep is the use of personal data by subsequent data users for a new purpose.

[149] <www.pcpd.org.hk/english/publications/files/GN_public_domain_e.pdf> accessed 19 October 2016.

[150] Law Reform Commission, 'Issues Paper on Cyber-crime affecting person safety, privacy and reputation including cyber-bullying (LRC IP 6-2014), <http://www.lawreform.ie/_fileupload/Issues%20Papers/ip6Cybercrime.pdf> accessed 20 April 2016.

5.35 It should be remembered that permanence and speed of online communications is a norm in this digital age. In addition, the anonymity that the Internet provides means that individuals are more unrestrained in their comments, postings, and communications, either disregarding or being indifferent to the repercussions of putting in the public domain, personal details and information of the other person. For example, posting on social media, the identification card of a person online, including the person's residential address, could expose that person to identity theft and could affect his or her personal safety.

5.36 If such actions amount to a serious breach of privacy, the question is whether the threshold of seriousness necessitates the criminalisation of such an action and what (if any) considerations should be taken into account in such an offence.

5(a) Is the action of revealing personal details or intimate actions (that do not amount to outraging modesty) in a one-off action and using cyber enabled technology, amounts to serious interference with a person's right to privacy?
5(b) If the above is answered in the affirmative, should the action be criminalised and what (if any) considerations should be taken into account in such an offence, to ensure a balance between freedom of expression and right to privacy of an individual?