Research Office
Legislative Council Secretariat

Information Note

Measures to address doxxing in selected places

IN09/19-20

1. Introduction

1.1 The emergence of online content hosts [1] provides a digital environment where personal information can be stored, accessed and disseminated electronically. Yet, data proliferation[2] has been abused by some netizens to cyberbully and cause harm to others. This has given rise to discussions about whether existing regulatory regimes are adequate to protect personal privacy and if not, whether any enhancements so introduced would impose excessive restrictions on other rights such as the freedom of speech and expression (e.g. disclosure of information in the public interest).

1.2 According to Article 19 of the International Covenant on Civil and Political Rights, the freedom of expression may be restricted to respect the right of others, e.g. the right to privacy. Nevertheless, such restrictions must be provided by the law, justified by legitimate aims, and proportionate to the interests to be protected. This approach to balancing personal privacy against the freedom of expression is commonly recognized by the human rights legislation in Hong Kong[3] and overseas places[4].

1.3 In Hong Kong, the balance between the freedom of expression and the right to privacy has been the subject of heated discussion since the outbreak of social unrest in June 2019. During the period, the personal information of some police officers, journalists and members of the public has reportedly been "doxxed", i.e. disclosed without their consent. As at

---

1 An online content host is a person who controls an online system, such as a website or app, where content can be posted and viewed.

2 Data proliferation refers to the large number of files and amount of data stored by entities such as governments, businesses, and online content hosts.

3 The Hong Kong Bill of Rights Ordinance (Cap. 383) safeguards the right to freedom of expression.

4 For example, the United Kingdom's Human Rights Act 1998 safeguards the right to freedom of expression. But the law states that this freedom "may be subject to formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society".

10 January 2020, the Office of the Privacy Commissioner for Personal Data ("PCPD") had received 4 400 related cases involving 17 online social platforms and 2 937 web links. Among the cases received, around 60% related to members of the public, 36% involved police officers and their family members,[5] and 4% affected government officials and public servants. There is also an added concern that personal data in the register of electors may be misused for doxxing.

1.4 While criminal doxxing may be prosecuted by the law, there are views that existing safeguards for personal data privacy may not be adequate to address the problem of doxxing. For instance, PCPD does not have the power to remove harmful content online, and can only render limited assistance to victims of doxxing. This has prompted the Government to consider amending the relevant legislation and enhancing PCPD's statutory powers to deter cyberbullying.

1.5 The prevalence of offensive online behaviours is no different in overseas places which have resorted to various approaches to address the problem. For instance, Australia and Canada have amended their general harassment offences to prosecute doxxing in technology neutral terms[6]. Germany introduced the Network Enforcement Act in 2017 requiring companies with two million registered users or above to comply with the duty of care to moderate harmful content[7]. In comparison, the United Kingdom ("UK") prosecutes doxxing under its existing data protection and communication laws. Nevertheless, it has recently put forth proposals for imposing a statutory duty of care on online content hosts to address harmful content or activity on their platforms.

1.6 In addition to introducing an offence on doxxing, Singapore has gone further with establishing a specialized court to expedite applications of civil remedies for the offence. Meanwhile, New Zealand has introduced a tiered redress regime consisting of voluntary content moderation of harmful content

---

[5] On 25 October 2019, the Secretary of Justice and the Commissioner of Police were granted an interim injunction to protect police officers and their families from doxxing by banning the publication of their personal details for harassment. The court has ordered that the injunction is to be continued until trial or further order. It has also clarified that the interim injunction does not prohibit the lawful act of news activity. See Hong Kong Police Force (2019).

[6] Technology neutral means that the same standard of criminal offence should apply regardless of the technology used to commit the offence.

[7] See Library of Congress (2019).

by online platforms, complaint resolution by an Approved Agency, and protection orders granted by the court.

1.7 In many overseas places, personal data in public registers such as the electoral register is subject to the same protection as personal data from other sources. For example, New Zealand's Public Register Privacy Principles set out restrictions on how data in public registers is used. As a further safeguard, voters with safety concerns may request their information to be removed from the electoral roll. The same safeguard for electoral registers is also found in Australia, Canada and the UK. In contrast, Singapore safeguards the information of voters by restricting public access to the electoral register.

1.8 At the request of Hon Alice MAK Mei-kuen, the Research Office has prepared this information note on measures to address doxxing in Hong Kong, with special reference to the work of PCPD and related cases heard by the court. The information note also studies the legislation to protect the public from doxxing in New Zealand and Singapore, covering issues such as the rationale for the legislative regimes, redress and remedies available, and safeguards against misuse of personal data in the electoral roll/register.

2. Measures to address doxxing in Hong Kong

2.1 The Personal Data (Privacy) Ordinance ("PDPO") (Cap. 486) is a technology neutral legislation regulating the collection, handling and disclosure of personal data. PDPO sets out the Data Protection Principles which prohibit the use of personal data for any new purpose which is not or is unrelated to the original purpose when collecting the data without the data subject's consent.[8, 9] Furthermore, it is a criminal offence under PDPO to disclose any personal data without the data owner's consent, provided that such disclosure causes psychological harm to the data subject.[10] Acts of cyberbullying or doxxing may fall under the scope of this offence. In order to ensure a balance of rights, it is a reasonable defence to argue that the disclosure is a news activity and/or is in the public interest.

---

8 Contravention of the principles in itself is not a criminal offence. However, PCPD may issue an enforcement notice requiring a data user to remedy or desist from such contravention.

9 In relation to personal data, "data subject" refers to the individual who is the subject of the data.

10 In relation to personal data, "data owner" means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data.

PCPD's actions on addressing doxxing

2.2 As an independent statutory body, PCPD is responsible for overseeing the enforcement of PDPO in Hong Kong. It has the statutory power to initiate investigations for suspected contraventions of PDPO. Simply put, doxxing cases in breach of the Data Protection Principles without causing psychological harm to the victims are regarded as non-criminal doxxing. PCPD may serve an enforcement notice after an investigation to direct a data user to remedy or desist from the contravention.[11] In contrast, doxxing cases which cause psychological harm to the victims either through intimidation or incitement are regarded as criminal doxxing. Criminal cases are referred to the Police Cyber Security and Technology Crime Bureau for further investigation. Since the outbreak of social unrest, PCPD had referred 1 402 cases of suspected criminal doxxing to the Police as at January 2020, resulting in eight arrests.[12]

2.3 PCPD has taken additional measures to deter doxxing. For instance, it has written to relevant online platforms requesting them to remove doxxing related content, as well as provide identifying information of the doxxers involved. For online platforms in overseas places, PCPD has also written to the relevant data protection authorities seeking cross-jurisdiction collaboration. Notwithstanding the above, PCPD's effort to address doxxing has been limited by the following:

(a) **limited compliance by online content hosts:** As at 10 January 2020, PCPD had written to 16 online platforms requesting the removal of 2 565 web links related to doxxing.[13] Among them, 1 725 or 67% of links were removed. PCPD has encountered difficulty with the remaining links because it does not have the power to order mandatory takedown. Some of the platforms also operate outside Hong Kong where PCPD has no jurisdiction;

---

[11] Non-compliance with an enforcement notice is an offence liable to a fine and/or imprisonment for up to two years.

[12] On 25 September 2019, the Police made prosecution for the first time of a man in connection with a criminal doxxing case.

[13] See Office of the Privacy Commissioner for Personal Data (2020).

(b) **narrow scope of assistance for victims:** PCPD may render assistance to victims through legal advice, mediation and legal representation prior to proceedings. However, PCPD does not have the authority to represent victims during legal proceedings, e.g. apply for an injunction requiring the removal of harmful content on the victim's behalf; and

(c) **lack of power to conduct criminal investigation:** PCPD may initiate an investigation upon receiving a complaint, or if there are reasonable grounds to believe that a breach of PDPO has occurred. Yet, PCPD does not have the power to conduct criminal investigation and prosecution for offences under its remit. It is also unable to issue prohibitive orders directing Internet intermediaries to provide information on anonymous doxxers.

2.4 At the meeting of the Panel on Constitutional Affairs on 20 January 2020, the Government responded to the above limitations of PCPD in handling doxxing. The Government stated that it is working jointly with PCPD to study possible amendments to PDPO with a view to strengthening the protection of personal data in Hong Kong. The amendments being considered include empowering PCPD to (a) conduct criminal investigation and prosecution; (b) impose direct administrative fines; (c) request the removal of doxxing content on online platforms; and (d) provide a broader range of legal assistance to victims.[14]

Access to personal data in public registers

2.5 In addition to the concerns over the adequacy of PDPO in personal data protection, there have been discussions in the community about the issue of restricting disclosure of personal data in the final register of electors ("final register") to curb doxxing. In 2015, PCPD conducted a review on 10 commonly used public registers, including the register of electors.[15]

[14] See Constitutional and Mainland Affairs Bureau (2020) and Office of the Privacy Commissioner for Personal Data (2020).

[15] In general, the personal data collected from a public register can only be used for its prescribed purposes, such as recording births and marriages or ascertaining whether a bankruptcy order has been made. The review found that the common public registers provided limited safeguards against potential misuse of personal data. See Office of the Privacy Commissioner for Personal Data (2015).

Following the recommendations made by the survey, a number of public registers have imposed safeguards to improve the protection of personal data privacy in the public registers. These include requiring data requesters to submit declarations of intended use in writing[16].

2.6 The rekindled discussion about the final register has been triggered by newfound concerns over the use of the names and principle residential addresses of voters contained therein for doxxing in recent months. At present, the final register is published each year by the Registration and Electoral Office. Upon publication, it is available for public inspection. Members of the public who wish to inspect the register are required to fill in an inspection form declaring the purpose for inspection. Furthermore, it is a criminal offence for any person to reproduce or transmit the information in the register.

2.7 In October 2019, the Junior Police Officers' Association ("JPOA") of the Hong Kong Police Force applied for judicial review to challenge the Electoral Affair Commission's practice of making the final register available for public inspection. JPOA argues that the practice infringes the registered electors' right to privacy. In contrast, some members of the public have cautioned that limiting access to the final register may adversely impact the free flow of information. For instance, news activity relies on information in the final register to provide oversight on matters of public interest.[17] Although the judicial review was dismissed initially, an interim injunction[18] was granted to suspend public inspection of the final register. On 8 April 2020, the court dismissed JPOA's appeal and the interim injunction is no longer in effect.

---

[16] Public registers which have adopted this measure include the Register of electors, Companies register and Bankruptcy register. See GovHK (2018).

[17] The Hong Kong Journalists Association applied to intervene in the judicial review by JPOA on the grounds that its involvement will provide a fuller consideration of other constitutional rights such as the freedom of the press. The application was granted by the High Court on 25 November 2019.

[18] The court considered that this would protect members of JPOA from doxxing without compromising the integrity of the election.

3. Measures to address doxxing in New Zealand

3.1 In New Zealand, cyberbullying was prosecuted by separate relevant laws[19] prior to the enactment of the Harmful Digital Communications Act ("HDCA") in 2015. In 2012, the New Zealand Law Commission reviewed existing laws on cyberbullying amid mounting concerns about the use of new communication technologies to cause harm.[20] The review concluded that the regulatory regime at that time was difficult to enforce and provided inadequate remedies, and that restrictions which were proportionate for traditional media mighty not be adequate for the Internet. The Law Commission hence recommended introducing specific legislation to mitigate the harms inflicted by offensive digital communications.

3.2 Following the Law Commission's recommendation, the New Zealand parliament passed HDCA with a significant majority in 2015. The Act introduces a specific criminal offence for cyberbullying, provides a broad range of civil remedies for affected victims, and establishes an Approved Agency which handles, mediates and resolves complaints.

Salient features of the Harmful Digital Communications Act

3.3 HDCA outlines 10 "communication principles" to provide guidance on what qualifies as a harmful digital communication. As shown in the **Table** below, doxxing may result in a breach of the principles if it involves the disclosure of sensitive personal information, or is deemed threatening, intimidating, menacing or grossly offensive. As discussed below, a person who suffers from a breach of the communication principles may complain to the online content host concerned or an Approved Agency, or seek remedies from the court. Serious cases may be referred to the police for criminal investigation and prosecution.

---

[19] Prior to HDCA, cyberbullying involving threats or intimidation were prosecuted by the Crimes Act 1961, Summary Offences Act 1981, Harassment Act 1997 or Telecommunications Act 2011.

[20] According to the Law Commission, new communication technologies can have effects which are more intrusive and more pervasive, and thus more hurtful, than many other forms of activity. For instance, it was found that up to 1 in 10 New Zealanders had some personal experience in harmful communication on the Internet. See Law Commission (2012).

Table — Communication principles under the Harmful Digital Communications Act

Communication principles	Basis in New Zealand law
1. A digital communication should not disclose sensitive personal facts about an individual.	• Tort of invasion of privacy; • Information principle 11 in the Privacy Act 1993; and • Intimate visual recording offences in the Crimes Act 1961.
2. A digital communication should not be threatening, intimidating, or menacing.	• Intimidation provisions in the Crimes Act 1961 and Summary Offences Act 981.
3. A digital communication should not be grossly offensive to a reasonable person in the complainant's position.	• New offence under HDCA.
4. A digital communication should not be indecent or obscene.	• Intimate visual recording offences in the Crimes Act 1961; and • Sexual grooming provisions in the Crimes Act 1961.
5. A digital communication should not be part of a pattern of conduct that constitutes harassment.	• Harassment Act 1977.
6. A digital communication should not make a false allegation.	• Tort of intentional infliction of emotional distress; • Law of false attribution; and • Law of defamation.
7. A digital communication should not contain a matter that is published in breach of confidence.	• Law of breach of confidence.
8. A digital communication should not incite or encourage anyone to send a message to a person with the intention of causing harm to that person.	• Inciting or counselling a person to commit an offence in the Crimes Act 1961; and • Incitement to suicide offence in the Crimes Act 1961.
9. A digital communication should not incite or encourage another person to commit suicide.	• Incitement to suicide offence in the Crimes Act 1961.
10. A digital communication should not denigrate a person by reason of his or her colour, race, ethnic or national origins, religion, gender, sexual orientation, or disability.	• Human Rights Act 1993.

Source: Ministry of Justice (2014).

Complaint process and civil remedies for victims

3.4 HDCA provides for a two-tier complaint handling process, which is an informal resolution scheme comprising (a) voluntary moderation of harmful content by online platforms; and (b) complaint resolution by an Approved Agency. Netsafe, an independent non-profit organization focused on online safety, has been appointed as the Approved Agency under HDCA entrusted with the statutory role to prevent and address online harassment.

3.5 Under the voluntary moderation of harmful content scheme, online content hosts are exempt from legal liability for any harmful content posted on their platforms by a third party if they follow the "safe harbour" provisions. These provisions are a set of rules requiring online platforms to handle doxxing-related complaints in an accessible and timely manner (**Appendix I**). Upon receiving a complaint,[21] the host is required to notify the author of the content within 48 hours. The content can be taken down under three scenarios, namely (a) with the author's consent; (b) the author does not reply; or (c) the online content host cannot reach the author. If the author refuses to take down the content after notification, the online content host is required to leave the content in place and inform the complainant within the next 48 hours.[22] The above procedure incentivizes online content hosts to moderate cyberbullying without requiring them to censor specific types of content.[23]

3.6 Complaints that are not resolved by the online content hosts can be brought to Netsafe. Alternatively, victims of cyberbullying can lodge their complaints directly with Netsafe, which is the port of first call for complainants before seeking remedies from the court. Under HDCA, Netsafe works as an impartial dispute resolution agency which investigates complaints and resolve differences between parties.[24] For instance, it can liaise with online content hosts on the victim's behalf and request the removal of posts that are clearly offensive.

---

[21] A complaint may be lodged by the complainant or by Netsafe on his or her behalf.

[22] Online content hosts also have the discretion to remove content in violation of their community standards. See Ministry of Justice (2016).

[23] However, the takedown system might encourage risk-averse hosts to take down too much content, which might hinder freedom of expression. See The Conversation (2015).

[24] Netsafe may decline to investigate if the content of the communication is unlikely to cause harm, or if its decision of investigating the complaint would be unlikely to uphold or enhance the communication principles.

3.7 Netsafe's service to handle cyberbullying, online abuse and online harassment was launched in November 2016. Since the inception of the service, Netsafe has received increased number of complaints. In 2019, Netsafe received a total of 3 377 reports relating to harmful digital communications, of which 212 cases were deemed to be qualifying complaints. Around 65% of qualifying complaints were resolved successfully.[25]

3.8 Victims who suffer from cyberbullying may apply for a range of remedies from the District Court. In order to prevent the court from being weighed down by meritless cases, it will only consider serious cases which have already lodged complaints at Netsafe.[26, 27] The courts may order a defendant to remove specific content, refrain from harmful conduct, or publish an apology or correction. It may also require an online content host to disable public access to specific content or reveal the identity of an anonymous offender. In deciding whether to grant a remedy, the court is required to take into account factors such as the level of harm caused, the vulnerability of the victim, the extent to which the content is spread, and whether the communication is in the public interest. These safeguards ensure that the remedies strike a balance between the prevention of harmful content and freedom of expression.

Criminal offence on doxxing

3.9 Prior to the enactment of HDCA, the law in New Zealand only criminalized threats or intimidation involving a risk to physical safety. The enactment of HDCA introduces an offence of causing harm by posting a digital communication[28]. HDCA defines "harm" as serious emotional distress[29], amid

---

[25] The remaining 35% of cases were either unresolved or referred to law enforcement bodies. Since Netsafe is not an enforcement body, it does not have the power to pursue follow-up action if a complaint is unresolved. See Netsafe (2019).

[26] Under HDCA, persons who consider themselves to be victims of cyberbullying must first lodge a complaint with NetSafe, which will then seek to settle the case through negotiation, mediation and persuasion. Failing that, court proceedings may be initiated. Applications made by the police to the district courts do not have to go through the above complaint process.

[27] An application for civil remedies can only be filed by victims, parents, guardians, school principals or the police.

[28] The offence carries a maximum penalty of two years' imprisonment or a fine of NZ$50,000 (HK$258,000).

[29] The New Zealand courts ruled in a 2016 case that serious emotional distress did not have to involve physical harm, but the victim must be more than merely annoyed or upset. See Gibson Sheat (2017).

the growing recognition in New Zealand that online communications causing serious emotional distress should also be deterred. For a person to be convicted of the offence, the prosecution is required to prove the intention to harm, and meet both objective and subjective tests. [30] This relatively narrow definition ensures that only severe cases of cyberbullying fall within its scope. Since the enactment of HDCA, the number of persons charged with this offence increased from 18 in 2015-2016 to 92 in 2018-2019.[31] The figures also include cases of cyberbullying and doxxing[32].

Appeal mechanism

3.10 Since Netsafe administers a voluntary complaint process without enforcement powers, its decisions cannot be appealed.[33] However, Netsafe must notify the complainant of his or her right to apply for a court order if it decides not to pursue further action on a complaint. In contrast, the District Court's civil and criminal rulings under HDCA can be appealed. A person may apply to vary or discharge a court order by submitting an interlocutory application with the grounds of appeal and an affidavit of supporting facts. Further appeals against both civil and criminal cases can be brought to the higher courts, where a technical adviser may be appointed to assist the judges in considering the case.[34]

Issues of concern

3.11 There have been concerns about the possible curtailment of freedom of expression by HDCA since the law came into place in 2015[35]. Nonetheless, the New Zealand Human Rights Commission[36] is satisfied that HDCA contains

---

30 The offence is committed if a digital communication is posted with the intent to cause harm, provided that such an act would cause harm to an ordinary person (i.e. objective test) and does indeed cause harm to the victim (i.e. subjective test). See Ministry of Justice (2014).

31 See Ministry of Justice (2020).

32 For instance, a woman was convicted in 2018 for disclosing the personal information and posting derogatory attacks against a sex worker. See Vice (2018).

33 The same applies to the complaints handled by online content hosts.

34 As at December 2017, there had been four cases of appeal against criminal sanctions under HDCA. See Williamson (2018).

35 See Dobson Hugo (2015).

36 The New Zealand Human Rights Commission is an independent crown entity working under the Human Rights Act 1993 to safeguard human rights in New Zealand. See Human Rights Commission (2014).

a number of safeguards to ensure a balance of rights. For instance, the Act expressly requires the court and Netsafe to act consistently with the rights and freedoms enshrined in the New Zealand Bill of Rights Act 1990. It also sets a relatively high legal threshold for the court to grant remedies and/or convict a person.

3.12 There are also suggestions that Netsafe's role should be enhanced to provide more efficient redress for victims.[37] Despite Netsafe's duty to resolve complaints, it has no statutory role to apply for remedies on the victims' behalf.[38] This may present a barrier for some complainants as they are left to seek remedies on their own. Furthermore, the judges of the District Court have suggested that Netsafe should screen all applications, including those made by complainants to the District Courts, and refer those substantial cases to the court.[39] This is to avoid (a) placing the onus on individuals to apply to the courts if the matter cannot be resolved by Netsafe; and (b) preventing the District Court from being burdened by meritless applications.

3.13 In addition, HDCA does not set any provisions governing offences committed outside New Zealand. When material is located on overseas websites but accessible in New Zealand, jurisdictional issues can arise for the courts and enforcement agencies. Under HDCA, the court may make a declaration that a communication breaches a communication principle[40]. According to the New Zealand government, this has no mandatory authority but would have significant persuasive power in relation to Internet intermediaries operating outside New Zealand's jurisdiction[41].

Safeguards for personal data in the electoral roll

3.14 In New Zealand, the identity information in public registers (including the electoral roll) is subject to protection as personal data. The Privacy Act in

---

37 See Panzic (2015).

38 According to the Ministry of Justice, Netsafe's role as an impartial mediator prevents it from applying for remedies on the complainant's behalf. See Ministry of Justice (2014).

39 See Chief District Court Judge for New Zealand (2014).

40 See New Zealand Legislation (2013a).

41 Large corporations like Google and Facebook have developed protocols for responding to authoritative requests from governments and law enforcement agencies for information about users, or to notices and takedown orders. Facebook's data policy, for example, states: "We access, preserve and share your information with regulators, law enforcement or others in response to a legal request (e.g. a search warrant, court order or subpoena) if we have a good-faith belief that the law requires us to do so". See New Zealand Government (n.d.).

New Zealand provides for a set of Public Register Privacy Principles which guide how information in public registers should be used. For instance, personal information in public registers should not be circulated electronically, and information from different registers should not be combined or re-sorted. However, these are only general guidelines that do not entail legal obligations.

3.15 The electoral roll is subject to additional safeguards on top of those mentioned above. In New Zealand, the name, address and occupation of an eligible voter are detailed in the electoral roll, which is generally available for public inspection in public libraries and electoral offices. However, voters with demonstrable safety concerns[42] may request their information to be moved to a confidential and unpublished roll. The applications must be supported by evidence such as copies of court protection orders, statements from the police, or letters of explanation.

4. Measures to address doxxing in Singapore

4.1 In November 2014, Singapore enacted the Protection from Harassment Act ("POHA") in an effort to provide a range of criminal sanctions and civil remedies against both online and offline harassment. Before that, harassment was already a crime in Singapore under the Miscellaneous Offences (Public Order and Nuisance) Act but it was not clear whether online harassment was covered under that Act. The passage of POHA was also in response to the concerns that victims of harassment had difficulty accessing adequate remedies. The new law gave victims of cyberbullying the option to avail of civil remedies.[43] In addition, the courts could grant a broader range of protection orders requiring harassers to desist from causing further harm to victims.[44]

---

[42] For instance, individuals may demonstrate safety concerns if their work or personal circumstances place them at risk, or if they are victims of domestic violence or harassment. See New Zealand Electoral Commission (2020).

[43] POHA does not set up a specific complaint scheme for victims of doxxing. The Personal Data Privacy Commission administers a complaint scheme for breaches on the collection, use or disclosure of personal data by an organization. However, the scheme does not cover breaches by individuals acting in a personal or domestic capacity. See Singapore Statutes Online (2012).

[44] As at 7 May 2019, there had been more than 1 700 prosecutions and 500 applications for protection order since the POHA came in force in November 2014. See Parliament of Singapore (2019).

4.2 Notwithstanding the enactment of POHA, there had been increasing cases of personal information being consolidated and published online to cause harassment. In one case, an expatriate banker was doxxed after posting derogatory comments about the poor on social media. His home address, place of work and mobile telephone number were disclosed by a group of netizens and he had to leave Singapore upon receiving death threats. This raised concerns over whether there was adequate protection for victims of doxxing under the existing legislative regime, especially in "pile on" situations where cyberbullying is committed by a group of netizens.

Amendments to the Protection from Harassment Act

4.3 In 2019, the Ministry of Law proposed further amendments to POHA to address the problem of doxxing. The amendment introduces new offences and criminal sanctions on doxxing[45]; expands the scope of redress for victims of cyberbullying; and establishes the specialized Protection from Harassment Court to expedite applications for redress. The amendment bill was passed by the parliament and became effective on 1 January 2020.

Criminal offences on doxxing

4.4 Two criminal offences were revised to cover doxxing under the amended POHA. The first offence involves the publication of identity information with the intent to cause harassment, alarm or distress. A person who posts identity information with the direct intent to cause harm to another may be liable. The second offence involves the publication of identity information to cause the fear of violence or facilitate the use of violence. A person may be liable if he or she posts identity information to facilitate a third party's threat of violence against a victim.[46] Taken together, these sanctions deter both direct acts of doxxing and disclosures of personal information in "pile on" situations.

---

[45] The original POHA which was enacted in 2014 did not expressly criminalize doxxing.

[46] The maximum penalty for the first offence is imprisonment for six months and/or a fine of S$5,000 (HK$28,700), whereas the maximum penalty for the second offence is imprisonment for twelve months and/or a fine of S$5,000 (HK$28,700). The penalty for both offences can be doubled for repeat offenders.

4.5 The Ministry of Law also provides some examples of doxxing to clarify its scope amid concerns that its criminal sanctions may be too broad. For instance, sharing an individual's person's personal information with the authorities or emergency services so that necessary action can be taken is not regarded as doxxing.[47] The examples provided are not exhaustive and whether there is a contravention depends on the context of each case.

Protection for victims of doxxing

4.6 Under POHA, the courts may grant various remedies to protect victims[48] from cyberbullying or doxxing. For instance, the court might issue the following four types of protection orders:

(a) stop-publication orders – requiring a publisher to take down an offending communication or false statement and prohibiting him or her from publishing any substantially similar content;

(b) disabling orders – requiring Internet intermediaries to disable access to specific content and/or reveal the identifying information of anonymous offenders;

(c) stop-and-desist orders – prohibiting the offender from pursuing any action in relation to the victim or any related persons as per the District Court's direction; and

(d) community orders – requiring the offender to attend counselling or psychiatric treatment as per the District Court's direction.

4.7 Protection orders are only issued if the court is satisfied, on the balance of probabilities[49], that an offence has been committed and the contravention is likely to continue. For cases which are likely to have a substantial adverse effect on the victim, an expedited protection order can be granted if there is prima facie evidence of contravention.[50] In general,

---

47 Other examples include posting a video of a person driving recklessly on the road on an online forum where people share snippets of dangerous acts of driving, with the intent to warn people to drive defensively. See Ministry of Law (2019a).

48 The protective measures can be extended to persons related to the victim such as family members.

49 The balance of probabilities is a legal standard where the court considers that, on the evidence, the occurrence of the event was more likely than not.

50 An expedited protection order remains in force for 28 days or until the hearing for a protection order commences, whichever is earlier. See Ministry of Law (2020).

applications for protection orders are processed within four weeks, whereas applications for expedited protection orders are heard within 24 to 72 hours.[51]

4.8 In order to further streamline the redress process, the amended POHA provides for the establishment of the Protection from Harassment Court, a specialized court which provides oversight over all criminal and civil matters under the Act. The Protection from Harassment Court is chaired by judges trained in harassment matters, and is designed to provide victims with readily accessible relief. For instance, victims of cyberbullying and doxxing may apply for protection orders using a simple claim form available in both online and offline formats. According to the Ministry of Law, this enables victims to navigate the civil redress procedure with ease, and without requiring the assistance of lawyers.

Appeal mechanism

4.9 The criminal and civil decisions made by the Protection from Harassment Court can be appealed. In the first instance, a person may seek to vary, suspend or cancel a protection order or expedited protection order by submitting an application with the supporting information. Further appeals against the Protection from Harassment Court's decisions can be brought to the High Court. However, there can be no further appeals against expedited protection orders.

Issues of concern

4.10 Unlike New Zealand's HDCA, Singapore's POHA does not have express provisions to ensure a balance of rights, or to provide exemptions for disclosures in the public interest. There are concerns that POHA may curtail the freedom of expression in Singapore. Despite the express legislative intent to protect "persons" against harassment and provide civil remedies to false statements of fact,[52] the Singapore government has attempted to argue that public agencies qualify as a "person" and are able to apply for protection under POHA[53].

---

[51] Expedited protection orders are typically heard within 48 to 72 hours, but may be heard within 24 hours if there is a risk of violence. See Ministry of Law (2019a).

[52] See Ministry of Law (2020).

[53] See Freedom on the Net 2018 (2018) and Human Rights Watch (2017).

4.11 In February 2015, the Ministry of Defence sought a stop-publication order against an article published in The Online Citizen, an independent online media platform. The article reported on statements made by an inventor over a patent rights dispute with the Ministry of Defence. Although the application for a court order was initially granted by the District Court, the decision was later overturned by the High Court in December 2015. The High Court ruled that public agencies could not be considered a "person" under POHA and therefore could not apply for protection from false statements. In January 2017, the Court of Appeal, Singapore's highest court, affirmed the judgment and dismissed the Ministry of Defence's appeal.

4.12 In addition, there had been concerns as to whether POHA would apply to cyberbullying outside Singapore prior to the enactment of the Act. Under section 17(6) of POHA, the courts have jurisdiction to try offences committed outside Singapore and to grant protection orders or expedited protection orders if the victim was in Singapore. This provision provides some extraterritorial reach for POHA to tackle the problem of overseas doxxing. As in many other overseas places, enforcement issues may arise in Singapore when the Internet intermediaries are operating in a foreign jurisdiction. Yet, there is no information in the public domain about the enforcement mechanism and whether the legal provisions are effective in curbing doxxing outside Singapore[54].

Safeguards for personal data in the register of electors

4.13 Similar to the case in New Zealand, identity information in the register of voters is subject to protection as personal data in Singapore. It is a criminal offence in Singapore to reproduce any personal information in the register of electors. Public inspection of the register is limited to a two-week period each year, during which citizens may verify their own personal particulars in the register. Furthermore, only political parties and election candidates can access the register for the purpose of communicating with electors. The Personal Data Protection Commission has issued a guideline advising political parties to handle the information in the register with care.[55]

---

[54] The Research Office has written to Singapore's Ministry of Law for information. As at the publication of this information note, the Ministry has not yet replied to the information request.

[55] For instance, it is recommended that political parties should put in place policies and procedures, and conduct the necessary training to ensure the appropriate handling of personal data in the register. See Personal Data Protection Commission (2017).

5. Concluding remarks

5.1 In Hong Kong, cyberbullying and doxxing have become more prominent following the outbreak of social unrest in June 2019. While criminal doxxing may be prosecuted under PDPO, there are concerns that the current data protection regime has limited remedies for victims of cyberbullying. Consequently, the Government is considering to empower PCPD to conduct criminal investigations, request the removal of doxxing content on online platforms, and provide a broader range of legal assistance to victims.

5.2 Both New Zealand and Singapore have specific offences to prosecute doxxing.[56] The salient features of the regulatory regimes adopted by New Zealand and Singapore to address doxxing are summarized in **Appendix II**. In New Zealand, the offence of causing harm by posting digital communication was introduced in 2015 to criminalize offensive online content which causes serious emotional distress. The offence has a relatively high criminal threshold to help strike a balance between the prevention of harmful content and freedom of expression. In contrast, Singapore amended its technology neutral harassment law in 2019 to prosecute doxxing. It is an offence to disclose any identity information with the intent to cause harassment, alarm or distress, or to facilitate the use of violence. These sanctions encompass a wider range of cyberbullying behaviour, including doxxing in "pile on" situations.

5.3 Specific remedies for victims of doxxing are also provided in New Zealand and Singapore. New Zealand opts for informal resolution mechanisms comprising content moderation by online content hosts and complaints handling by the Approved Agency, Netsafe. Netsafe seeks to settle the case through negotiation, mediation and persuasion. Failing that, court proceedings may be initiated. In contrast, civil redress in Singapore is administered solely by the Protection from Harassment Court, a specialized court that provides an accessible and inexpensive means to apply for remedies. Expedited remedies can be granted within 24 to 72 hours so that victims suffering from serious abuse can receive timely protection.

[56] In both New Zealand and Singapore, it is the police's responsibility to conduct criminal investigation and prosecution.

5.4 Legislating on doxxing inevitably raises concerns over its possible curtailment of the freedom of expression. In this regard, New Zealand has provided a number of safeguards to balance reduction of harm with people's right to freedom of expression. These include that:

(a) the statutory agency must follow the 10 "communication principles" set out in HDCA when deciding whether it should request the taking down of any harmful digital communication;

(b) the relevant parties must act consistently with the freedoms contained in the New Zealand Bill of Rights Act 1990;

(c) the court is required to consider whether an allegedly harmful communication is in the public interest before granting protection orders, and its civil and criminal decisions can be appealed; and

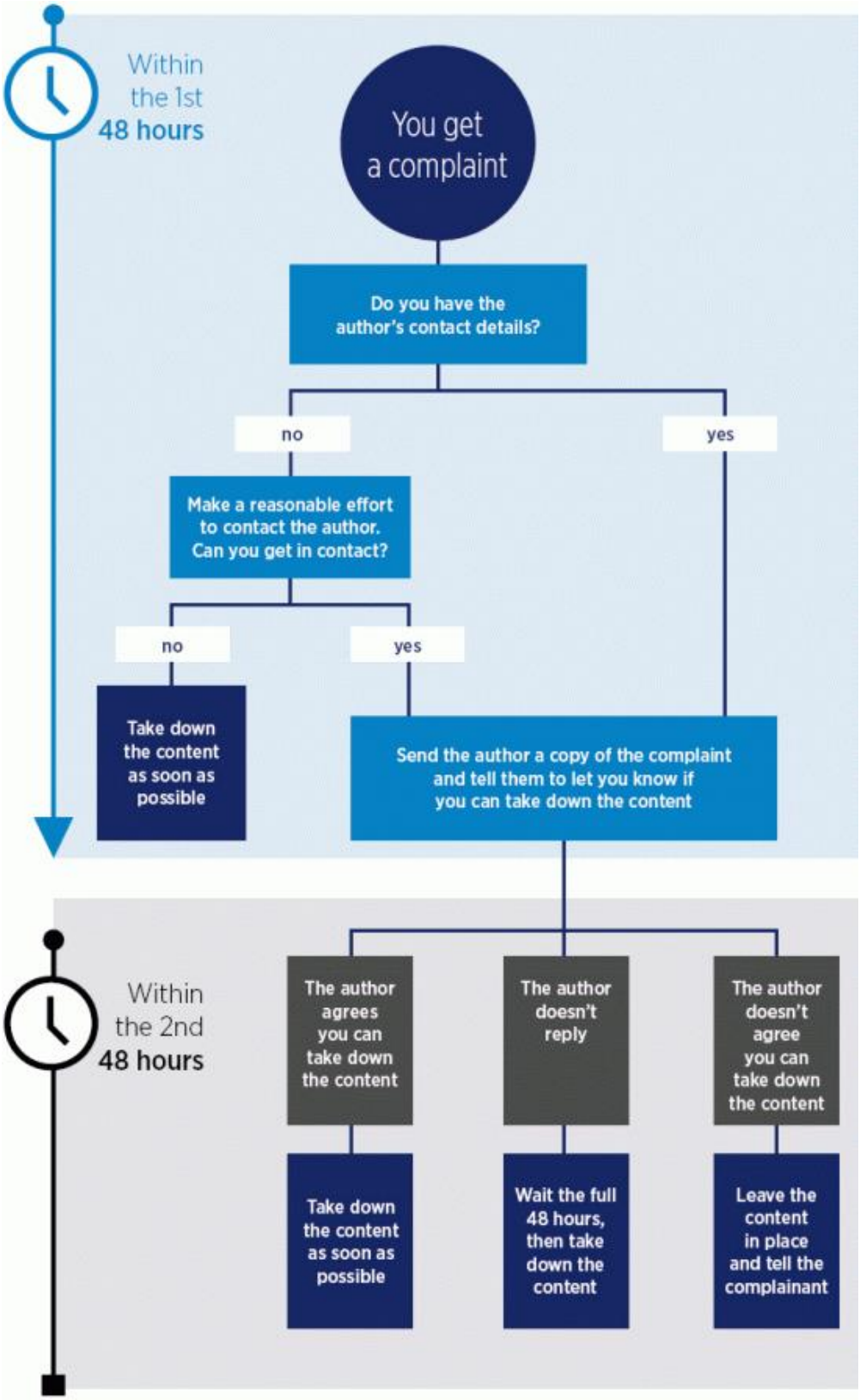
(d) the government has included a "safe harbour" provision in HDCA for third parties who host online content. While regulated by HDCA, the online content hosts can protect themselves against legal liability through a "notice and takedown" system for allegedly harmful material.

5.5 Unlike New Zealand, Singapore has not set out any provision in its POHA to balance between the prevention of harmful content and freedom of expression, or provide for exemptions for disclosures in the public interest. Nevertheless, the civil and criminal decisions by the Protection from Harassment Court can be appealed. There is also the further safeguard that public agencies could not be considered a "person" under POHA and therefore could not apply for protection from harassment.

5.6 In Hong Kong, the prominence of doxxing has also given rise to concerns that the information in the register of electors may be misused for doxxing. At present, public inspection of the register is suspended pending the result of judicial review. By comparison, both New Zealand and Singapore have measures in place to safeguard data privacy in the electoral roll/register. In New Zealand, voters with demonstrable safety concerns may apply for their information to be moved to an unpublished and confidential roll. In Singapore, public inspection of the register is time-limited, and citizens are only allowed to verify their own personal particulars.

Appendix I

Flow chart of the "safe harbour" provisions



Source: Ministry of Justice (2016).

Appendix II

Regulation of doxxing in Hong Kong, New Zealand and Singapore

	Hong Kong	New Zealand	Singapore
A. Background information			
Extent of cyberbullying and doxxing	• 4 400 reported cases of doxxing and cyberbullying since 14 June 2019.	• Around 1 in 10 New Zealanders had some experience of cyberbullying before legislation.	• Around three out of four children and teenagers had reportedly been victims of cyberbullying before the amended legislation.
Legislation against doxxing	• Personal Data (Privacy) Ordinance ("PDPO").	• Harmful Digital Communications Act 2015 ("HDCA").	• Protection from Harassment Act ("POHA").
Year enacted	• Enacted in 1995 and amended in 2012.	• Enacted in 2015.	• Enacted in 2014 and amended in 2019.
Purpose of the legislation	• Protect the privacy of personal data.	• Deter, prevent and mitigate harm caused to individuals by digital communications (HDCA defines harm as serious emotional distress); and • Provide victims of harmful digital communications with a quick and efficient means of redress.	• Protect individuals from offline and online harassment by introducing offences and providing civil remedies.
Responsible authority	• Office of the Privacy Commissioner for Personal Data ("PCPD").	• Netsafe, the Approved Agency under HDCA.	• Protection from Harassment Court.

Regulation of doxxing in Hong Kong, New Zealand and Singapore

	Hong Kong	New Zealand	Singapore
B. Criminal sanctions against doxxing			
Criminal offence against doxxing	• Section 64(2) of PDPO. • A person is liable if he or she discloses any personal data of a data subject which was obtained from a data user without the data user's consent, and such disclosure causes psychological harm to the data subject.	• Section 22 of HDCA. • A person is liable if (a) the person posts a digital communication with the intention to cause harm to a victim; (b) such an act would cause harm to an ordinary reasonable person in the victim's position; and (c) such an act causes harm to the victim.	• Sections 3(1) and 5(1A) of POHA. • A person is liable if he or she publishes any identity information with the intent (a) to cause harassment, alarm or distress against another person; (b) to cause the victim to believe that unlawful violence will be used against the victim or any other person; or (c) to facilitate the use of unlawful violence against the victim or any other person.
Maximum penalty	• Imprisonment of five years and/or fine of HK$1,000,000.	• Imprisonment of two years or a fine of NZ$50,000 (HK$258,000) for an individual. • A fine of NZ$200,000 (HK$1,033,000) for a body corporate.	• Imprisonment of 12 months or a fine of S$5,000 (HK$28,700). • The court may issue an enhanced punishment not exceeding twice the maximum penalty for repeated offences or offences against vulnerable persons.
Threshold for prosecution	• The offence involves the need to prove psychological harm as well as unlawful obtaining of personal data from a data user.	• The offence has a relatively high threshold due to the need to prove intent, objective harm and subjective harm. Harm is defined narrowly as serious emotional distress.	• The offence has a lower threshold due to the need to prove intent and objective harm only. Harm is defined more broadly to include (a) physical harm; (b) harassment, alarm or distress; or (c) being caused to believe that unlawful violence will be used against the victim.

Regulation of doxxing in Hong Kong, New Zealand and Singapore

	Hong Kong	New Zealand	Singapore
B. Criminal sanctions against doxxing (cont'd)			
Any defences to ensure the balance of rights	• Yes. • A person charged with the offence may rely on a list of defences, including that the disclosure was in the public interest and/or for the purpose of a news activity.	• Yes. • Under HDCA, the court and Approved Agency must act consistently with the rights and freedoms contained in the New Zealand Bill of Rights Act 1990. • The relatively high threshold for the offence ensures that the prevention of harm is weighed proportionately against constraints on the freedom of expression.	• No. • A person charged with the offence can only rely on the defence that his or her conduct was reasonable.
C. Other safeguards for victims of doxxing			
Any complaint schemes for victims of doxxing	• Yes. • PCPD handles complaints for privacy abuses relating to personal data. Depending on the case, it may resolve disputes through conciliation, issue enforcement notices against data users after investigation, and refer criminal cases to the police.	• Yes. • Netsafe administers a scheme to investigate and resolve complaints for harmful digital communications. • Victims must lodge a complaint with Netsafe before applying for remedies from the court.	• No. • For a breach on the collection, use or disclosure of personal data by an organization, complaints may be brought to the Personal Data Privacy Commission. However, this does not cover individuals acting in a personal or domestic capacity.

Regulation of doxxing in Hong Kong, New Zealand and Singapore

	Hong Kong	New Zealand	Singapore
C. Other safeguards for victims of doxxing (cont'd)			
Any specific remedies for victims of doxxing	• No. • Victims can apply for general injunction orders from the court.	• Yes. • Victims may apply to the court for remedies. The range of remedies includes ordering a defendant to remove specific content, refrain from harmful conduct, and/or publish an apology or correction. • The court may also instruct an online content host to disable public access to specific content and/or reveal the identity of an anonymous offender.	• Yes. • Victims may apply for protection orders from PHC to prohibit the offender from pursuing harassing actions, stop the publication of or disable access to offending communications, require the identity of anonymous offenders to be revealed and/or require the offender to attend counselling. • In general, applications for expedited protection orders are heard within 24 to 72 hours, whereas protection orders are processed within four weeks.
Any specific provisions for online content hosts	• No. • PCPD does not have the power to order online content hosts to remove doxxing-related content.	• Yes. • The "safe harbour" provisions provide an accessible complaint process which can be implemented on online platforms. Online content hosts complying with these rules are exempt from liability for harmful content posted by a third party.	• Yes. • Online content hosts may also be required to comply with specific orders issued by PHC.

Regulation of doxxing in Hong Kong, New Zealand and Singapore

	Hong Kong	New Zealand	Singapore
C. Other safeguards for victims of doxxing (cont'd)			
Any appeal mechanism	• Yes. • Appeals may be lodged to the Administrative Appeals Board against PCPD's enforcement decisions, such as termination of an investigation.	• Yes. • Interested parties may apply to vary or discharge a court order through an interlocutory application. • Further appeals against civil and criminal decisions can be brought to the higher courts.	• Yes. • Interested parties may apply to vary, suspend or cancel a protection order or expedited protection order. • Further appeals against civil and criminal decisions can be brought to the higher courts. However, expedited protection orders cannot be appealed.
D. Safeguards for personal data in electoral registers			
Relevant legislation and/or regulation	• Personal Data (Privacy) Ordinance; and • Electoral Affairs Commission (Registration of Electors) (Legislative Council Geographical Constituencies) (District Council Constituencies) Regulation.	• Privacy Act 1993; and • Electoral Act 1993.	• Parliamentary Elections Act.

Regulation of doxxing in Hong Kong, New Zealand and Singapore

	Hong Kong	New Zealand	Singapore
D. Safeguards for personal data in electoral registers (cont'd)			
Public inspection of electoral register	• The final register of electors is available for public inspection after publication. Requesters are required to fill in a form declaring the purpose for inspection. • An interim injunction was granted in October 2019 suspending public inspection of the register.	• The electoral roll is generally available for public inspection at public libraries and electoral offices.	• Public inspection of the register of electors is available for a two-week period each year. Citizens can only verify their own personal particulars in the register.
Measures to safeguard personal data in electoral registers	• It is a criminal offence for any person to reproduce or transmit the information in the register.	• Voters with demonstrable safety concerns may request their information to be moved to a confidential and unpublished roll. • It is an offence to supply in electronic form the information in the electoral roll for an unauthorized purpose.	• There are guidelines advising candidates to handle information in the register with due care. • It is a criminal offence to reproduce information in the register via electronic or other means.

References

Hong Kong

1. Constitutional and Mainland Affairs Bureau. (2020) *Review of the Personal Data (Privacy) Ordinance*. LC Paper No. CB(2)512/19-20(03). Available from: https://www.legco.gov.hk/yr19%2D20/english/panels/ca/papers/ca20200120cb2-512-3-e.pdf [Accessed April 2020].

2. Hong Kong e-Legislation. (2017) *Cap. 383 Hong Kong Bill of Rights Ordinance*. Available from: https://www.elegislation.gov.hk/hk/cap383 [Accessed April 2020].

3. Hong Kong e-Legislation. (2018) *Cap. 486 Personal Data (Privacy) Ordinance*. Available from: https://www.elegislation.gov.hk/hk/cap486?xpid=ID_1438403262675_004 [Accessed April 2020].

4. Hong Kong e-Legislation. (2019) *Cap. 541A Electoral Affairs Commission (Registration of Electors) (Legislative Council Geographical Constituencies) (District Council Constituencies) Regulation*. Available from: https://www.elegislation.gov.hk/hk/cap541A!en [Accessed April 2020].

5. Hong Kong Police Force. (2019) *Interim Injunction Order of the High Court (HCA 1957/2019) – Doxxing and Harassment against Police Officers, Special Constables and their Families*. Available from: https://www.police.gov.hk/ppp_en/03_police_message/iio_1957.html [Accessed April 2020].

6. GovHK. (2018) *LCQ17: Promoting opening up of data*. Available from: https://www.info.gov.hk/gia/general/201811/07/P2018110700424.htm [Accessed April 2020].

7. GovHK. (2019) *Injunction of public inspection of 2019 Final Registers of Electors/Voters*. Available from: https://www.info.gov.hk/gia/general/201910/22/P2019102200741.htm [Accessed April 2020].

8. GovHK. (2020) *LCQ2: Measures against doxxing*. Available from: https://www.info.gov.hk/gia/general/202001/08/P2020010800579.htm [Accessed April 2020].

9. *Office of the Privacy Commissioner for Personal Data*. (2020) Available from: https://www.pcpd.org.hk/index.html [Accessed April 2020].

10. Office of the Privacy Commissioner for Personal Data. (2015) *Survey of Public Registers Maintained by Government and Public Bodies*. Available from: https://www.pcpd.org.hk/english/resources_centre/publications/surveys/files/survey_public_registers.pdf [Accessed April 2020].

11. *Should Hong Kong Legislate on Cyberbullying? If so, how?* (2015) Available from: https://www.hkreform.gov.hk/en/docs/essay21_2015.pdf [Accessed April 2020].

New Zealand

12. Chief District Court Judge for New Zealand. (2014) *Submission on Behalf of the Judges of the District Courts*. Available from: https://www.parliament.nz/resource/en%2DNZ/50SCJE_EVI_00DBHOH_BILL12843_1_A380123/318f6cdddb0b1ab18858b37a543652afda6ac0c0 [Accessed April 2020].

13. Dobson, H. (2015) *Facebook hosts and third party posts: defamation in the Internet age.* Available from: https://www.otago.ac.nz/law/otago451213.pdf [Accessed April 2020].

14. Gibson Sheat. (2017) *The Harmful Digital Communications Act – Cyberbullies Beware*. Available from: https://www.gibsonsheat.com/Articles/Litigation/The+Harmful+Digital+Communications+Act+-+Cyberbullies+Beware.html [Accessed April 2020].

15. Human Rights Commission. (2014) *Harmful Digital Communications Bill*. Available from: https://www.parliament.nz/resource/en%2DNZ/50SCJE_EVI_00DBHOH_BILL12843_1_A373540/6cc6501e81a46414d7754a22d4e5a17bfd1afe2f [Accessed April 2020].

16. Law Commission. (2012) *Harmful Digital Communications: The Adequacy of the Current Sanctions and Remedies*. Available from: https://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC%20MB3.pdf [Accessed April 2020].

17. Library of Congress. (2019) *Erasure of Online Information: New Zealand*. Available from: https://www.loc.gov/law/help/erasure-online-info/newzealand.php [Accessed April 2020].

18. Ministry of Justice. (2014) *Harmful Digital Communications Bill: Departmental Report for the Justice and Electoral Committee*. Available from: https://www.parliament.nz/resource/en-NZ/50SCJE_ADV_00DBHOH_BILL12843_1_A387162/5eed063f4373109478ee70bbfdf1a96747aa2719 [Accessed April 2020].

19. Ministry of Justice. (2016) *Safe harbour provisions*. Available from: https://www.justice.govt.nz/justice-sector-policy/key-initiatives/harmful-digital-communications/safe-harbour-provisions/ [Accessed April 2020].

20. Ministry of Justice. (2020) Available from: https://www.justice.govt.nz/ [Accessed April 2020].

21. Netsafe. (2019) *Annual Report 2018/2019*. Available from: https://www.netsafe.org.nz/wp-content/uploads/2019/12/2019-Annual-Report-R174WEB-1.pdf [Accessed April 2020].

22. New Zealand Electoral Commission. (2020) Available from: https://vote.nz/ [Accessed April 2020].

23. New Zealand Government. (n.d.) *FAQs – Harmful Digital Communications Bills*. Available from: https://www.beehive.govt.nz/sites/default/files/FAQs_Harmful_Digital_Communications_Bill.pdf [Accessed April 2020].

24. New Zealand Legislation. (2013a) *Harmful Digital Communications Bill 168-1.* Available from: http://www.legislation.govt.nz/bill/government/2013/0168/6.0/whole.html#DLM5711801 [Accessed April 2020].

25. New Zealand Legislation. (2013b) *New Zealand Bill of Rights Act 1990*. Available from: http://www.legislation.govt.nz/act/public/1990/0109/latest/DLM224792.html [Accessed April 2020].

26. New Zealand Legislation. (2020) *Electoral Act 1993*. Available from: http://www.legislation.govt.nz/act/public/1993/0087/latest/DLM307519.html [Accessed April 2020].

27. Panzic, S. F. (2015) *Legislating or E-Manners: Deficiencies and Unintended Consequences of the Harmful Digital Communications Act*. Available from: http://www.nzlii.org/nz/journals/AukULawRw/2015/11.pdf [Accessed April 2020].

28. Parliamentary Counsel Office. (2015) *Harmful Digital Communications Act 2015*. Available from: http://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html [Accessed April 2020].

29. The Conversation. (2015) *Tackling the trolls: how New Zealand raised the bar with its new laws.* Available from: https://theconversation.com/tackling-the-trolls-how-new-zealand-raised-the-bar-with-its-new-laws-44691 [Accessed April 2020].

30. *Reserve Bank of New Zealand.* (2020) Available from: https://www.rbnz.govt.nz/ [Accessed April 2020].

31. Vice. (2018) *A New Zealand Woman was Charged for Doxing a Sex Worker Online*. Available from: https://www.vice.com/en_us/article/mbygqp/new-zealand-woman-charged-for-doxing-a-sex-worker-online [Accessed April 2020].

Singapore

32. Bird & Bird. (2019) *Legal Update: New Measures to Tackle Online Harassment and Online Falsehoods*. Available from: https://www.twobirds.com/~/media/pdfs/singapore/2019/bird--bird-atmd-legal-update-new-measures-to-tackle-online-harassment-and-online%2Dfalsehoods.pdf?la=en&hash=1926FB0E144F3B0AC3C0D4CBE883469BDE05B7CF [Accessed April 2020].

33. Court of Appeal of the Republic of Singapore. (2017) *Civil Appeal No 26 of 2016*. Available from: https://www.supremecourt.gov.sg/docs/default-source/module-document/judgement/ca26-2016-ca27-2016--2017-sgca-6(ed)-tingfinal3-16jan17-pdf.pdf [Accessed April 2020].

34. *Elections Department Singapore.* (2020) Available from: https://www.eld.gov.sg/ [Accessed April 2020].

35. Freedom on the Net 2018. (2018) *Singapore*. Available from: https://freedomhouse.org/report/freedom-net/2018/singapore [Accessed April 2020].

36. Goh, Y. & Yip, M. (2014) *The Protection from Harassment Act 2014: Legislative Comment*. Available from: https://ink.library.smu.edu.sg/sol_research/1394/ [Accessed April 2020].

37. Human Rights Watch. (2017) *"Kill the Chicken to Scare the Monkeys": Suppression of Free Expression and Assembly in Singapore*. Available from: https://www.hrw.org/report/2017/12/12/kill-chicken-scare-monkeys/suppression-free-expression-and-assembly-singapore [Accessed April 2020].

38. Library of Congress. (2019) *Laws Protecting Journalists from Online Harassment: Singapore*. Available from: https://www.loc.gov/law/help/protecting-journalists/singapore.php [Accessed April 2020].

39. Ministry of Law. (2019a) *Enhancements to the Protection from Harassment Act*. Available from: https://www.mlaw.gov.sg/news/press-releases/enhancements-to-the-protection-from-harassment-act-poha [Accessed April 2020].

40. Ministry of Law. (2019b) *Written answer by Minister for Law, K Shanugam, to Parliamentary Question on Protection Orders*. Available from: https://www.mlaw.gov.sg/news/parliamentary-speeches/written-answer-by-minister-for-law-k-shanmugam-to-pq-on-protection-orders [Accessed April 2020].

41. Ministry of Law. (2020) *Protection from Harassment Act*. Available from: https://sso.agc.gov.sg/Act/PHA2014 [Accessed April 2020].

42. Parliament of Singapore. (2019) *Protection from Harassment (Amendment) Bill: Speech by the Senior Minister of State for Law*. Available from: https://sprs.parl.gov.sg/search/sprs3topic?reportid=bill-362 [Accessed April 2020].

43. Personal Data Protection Commission. (2017) *Advisory Guidelines on the Application of Personal Data Protection Act to Election Activities*. Available from: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/advisory-guidelines-on-application-of-pdpa-to-election-activities---080817.pdf [Accessed April 2020].

44. Singapore Statutes Online. (2011) *Parliamentary Elections Act (Chapter 218)*. Available from: https://sso.agc.gov.sg/Act/PEA1954 [Accessed April 2020].

45. Singapore Statutes Online. (2012) *Personal Data Protection Act 2012*. Available from: https://sso.agc.gov.sg/Act/PDPA2012 [Accessed April 2020].

46. Singapore Statutes Online. (2020) *Constitution of the Republic of Singapore*. Available from: https://sso.agc.gov.sg/Act/CONS1963 [Accessed April 2020].

47. State Courts Singapore. (2019) *An Overview of the Protection from Harassment Act*. Available from: https://www.statecourts.gov.sg/cws/FillingForHarassment/Pages/Filing-for-Protection-from-Harassment---at-a-glance.aspx [Accessed April 2020].

48. Workers' Party. (2014) *Protection from Harassment Bill – MP Pritam Singh*. Available from: http://www.wp.sg/protection-from-harassment-bill-mp-pritam-singh/ [Accessed April 2020].

Others

49. Department for Digital, Culture, Media & Sport. (2019) *Online Harms White Paper*. Available from: https://www.gov.uk/government/consultations/online-harms-white-paper [Accessed April 2020].

50. Law Commission. (2018) *Abusive and Offensive Online Communications: A Scoping Report*. Available from: https://www.lawcom.gov.uk/abusive-and-offensive-online-communications/ [Accessed April 2020].

51. Library of Congress. (2019) *Laws Protecting Journalists from Harassment*. Available from: https://www.loc.gov/law/help/protecting-journalists/index.php [Accessed April 2020].

52. Legislation.gov.uk. (1998) *Human Rights Act 1998*. Available from: http://www.legislation.gov.uk/ukpga/1998/42/contents [Accessed April 2020].

53. United Nations Human Rights Office of the High Commissioner. (1976) *International Covenant on Civil and Political Rights*. Available from: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx [Accessed April 2020].

Prepared by Charlie LAM
Research Office
Information Services Division
Legislative Council Secretariat
23 April 2020
Tel: 2871 2146