The Cyber Social Phenomenon of Doxing: An Examination of Hong Kong's Anti-doxing Law

December, 2022

University of Glasgow: 2573321U

Dublin City University: 20109440

Charles University of Prague: 19049672

Presented in partial fulfilment of the requirements for the Degree of

International Master in Security, Intelligence and Strategic Studies

Word Count:	**23,934 words**
Supervisor:	**Dr. Julia Berg**
Date of Submission:	**15.December.2022**

Abstract

Doxing is a relatively new practice and phenomenon that emerged within the cyberspace, and there have been limited studies providing insights into this practice, especially concerning the legal measures available to address this practice. Hong Kong has recently experienced a widespread doxing phenomenon in light of social unrests stemming from the 2019 protest movement, and as a response, has introduced a legislative amendment to address this issue. This research paper aims to investigate and examine doxing and its effects in Hong Kong, as well as to investigate and understand how doxing is legally addressed in Hong Kong. It specifically examines the legislative text of the 2021 Amendment as well as other governmental publications in order to answer to three research questions: 1) What are the challenges that doxing posed to law enforcement?; 2) How has doxing in Hong Kong been addressed by the 2021 Amendment?; and 3) What are law enforcement's response to doxing after legal measures were introduced to address doxing? This research study observed the challenges that law enforcement faced before the 2021 Amendment, legal measures that were introduced, and how law enforcement responded to doxing after the 2021 Amendment. These points serve as a basis for discussion on the literature on doxing and its relevance to actual application in Hong Kong and future studies on doxing.

Table of Contents

List of Abbreviation

HKP	Hong Kong Police
HKPCPD	Hong Kong's Privacy Commissioner for
PDPO	Personal Data (Privacy) Ordinance

Chapter 1: Introduction

On a September evening in 2019, Isaac Cheng made his usual routine of returning home to his apartment (Adams & Lytvynenko, 2019). As he approached the entrance to his Hong Kong apartment, the then 19 years old Cheng took note of three strangers standing nearby but thought no more of it as he unlocked his front door and stepped into his apartment (Adams & Lytvynenko, 2019). Just as he was doing so, one of the three men suddenly punched Cheng's face (Adams & Lytvynenko, 2019). Stunned by the unexpectedly assault, Cheng recalled barely having the time to process what was happening amidst the chaos of profanities that were being shouted at him when he was again struck in the face (Adams & Lytvynenko, 2019). It was the beginning of a short, but traumatic few minutes of physical assault on Cheng by three strangers whom he had never known nor met before this incident (Adams & Lytvynenko, 2019). The attack only stopped when the commotion attracted the attention of a neighbour who yelled out from a window, scaring away the three attackers (Adams & Lytvynenko, 2019).

Cheng – also the vice chairman to a pro-democracy organization in Hong Kong called 'Demosisto' – later expressed his suspicion that the attack may have been related to his role in the then on-going protest movement within Hong Kong (Adams & Lytvynenko, 2019). However, this attack may not have been possible had Cheng not been 'doxed' only recently prior to the assault. The 'doxing' incident in late August had exposed Cheng's personal data, including his various social media accounts, his phone number, and his home address – where the assault took place (Adams & Lytvynenko, 2019). The 'doxer(s)' had compiled Cheng's personal data, alongside the personal data of numerous other protesters and published them on a website which had since been removed (Adams & Lytvynenko, 2019).

In the aftermath of the assault, Cheng and his family members had expressed fears and concerns for their safety in a city that was then in turmoil (Adams & Lytvynenko, 2019). Cheng, as well as other protesters, had not been the only ones who were targeted. As the protests had continuously escalated into violence, other relevant parties such as journalists and police officers also became the doxing targets as well (Hale, 2019). Journalists reporting on the 2019 Hong Kong protests have expressed fear of having their personal data being publicised and used as a leverage to coerce them into 'self-censorship' as well as simply used to stalk, harass, or harm them in the real world (Hale, 2019; Tsui, 2020). In addition, as some police officers had taken to wear casual outfits to blend in with the crowds of protesters as the protests began to escalate more frequently into violence, they had also become the prime doxing targets by the protesters (Hale, 2019; Purbrick, 2019; Tsui, 2020). Not only were personal data on the police officers themselves being publicised, and used to harass and harm them in the real-world, personal data of family members or close affiliates of these police officers were also being publicised – essentially condemning them to the same potential dangers to their privacy and safety by association (Cheung, 2021; Purbrick, 2019).

Similar to protesters like Cheng, the personal data of the targeted journalists and police officers were publicised on the internet across website such as 'LIHKG', a Hong Kong based web forum which gained tremendous popularity during the 2019 protest movement (Purbrick, 2019). The LIHKG forum was the main platform where doxed information was being disclosed and shared among online citizens, or 'netizens' (Purbrick, 2019). It had also been described as similar to 'Reddit' – a web forum which was similarly utilised in the several doxing incidents, including the doxing of suspects from the 2013 'Boston Bombing Marathon' and the infamous 'Gamergate' incident (Cheung, 2021; MacAllister, 2017). These doxing incidents illustrate that what Cheng was experiencing was far from an isolated case.

With the borderless nature of the cyberspace and how quickly information travels and spreads across the cyberspace, doxing goes beyond these high-profile cases. Doxing, as a social phenomenon, has become so prevalent in the cyberspace that it can happen anywhere and to anyone (Douglas, 2016), and more often than not, without the realisation that it was occurring. However, the understanding of this social phenomenon is still relatively undeveloped given that formal research on this subject were only conducted within the last decade.

The Cambridge's definition of doxing refers to "the action of finding or publishing private information about someone on the internet without their permission, especially in a way that reveals their name, address, etc." (Cambridge Dictionary, 2022), whereas the Oxford's definition refers to "[a]n online practice of exposing personal data about others which had previously been kept private" (Oxford Reference, 2022). Originally, the term 'dox' was coined as an alternative spelling of the term 'doc' which is an abbreviation of the word 'document', specifically used in the context of the phrase 'dropping docs' (Anderson & Wood, 2021; Cheung, 2021; Douglas, 2016; MacAllister, 2017). The first usage of the term can be traced back to the early 1990s culture of online hackers whereby rival hackers searched for and disclosed personal data of other rival hackers (Cheung, 2021; MacAllister, 2017). Although the intentions or motivations behind this practice vary, it has come to be understood as having an underlying malicious or harmful connation, as doxing would essentially strip away the veil of anonymity offered by the cyberspace, and leave the doxing target visible to the scrutiny of the public within the cyberspace (Cheung, 2021; Douglas, 2016), and by extent, leaving them vulnerable to malicious actors.

As the cyberspace evolved overtime, so too did doxing. Cheung (2021) observes the changes of this practice from being prevalent just within the small circle of online hackers to a more mainstream usage as it grew into more recognition among

the general public. This shift saw doxing becoming more of a mass or collective phenomenon (Cheung, 2021), whereby information is not just being actively searched for and published, but also circulated by the effort of the mass through media sharing which can lead to a state of 'context collapse'[1] (Lee, 2022). This state of context collapse enables the doxing target to be framed into any narrative, mainly as dictated by popular beliefs (Lee, 2022). In such situations, the doxed information can be used to harm the target, regardless of whether they are actually guilty or just simply an innocent party (Lee, 2022). This mainstream recognition of this practice was due to the media coverage of the online hacktivism movement, spearheaded at the time by an online hacktivist collective known as 'Anonymous' (Anderson & Wood, 2021). Despite garnering more interest, studies and literatures on doxing are still relatively new and limited.

As doxing has been mainly perceived as a social issue, studies on this subject have been mainly limited towards analysis of the social and technological implications of this online practice. Despite varying in nature across time and places, a general consensus can be gauged among scholars and researchers of digital vigilantism and doxing whom have called doxing unethical and even argued that some cases are flagrant violations of the law (Anderson & Wood, 2021; Douglas, 2016; Fish & Follis, 2016; Smallridge & Wagner, 2019). The primary focal points within the literature on doxing have been on how the practice has been weaponised as a tool for social control, the motives and objectives of the perpetrators, the implications it has for the victims (Anderson & Wood, 2021; Trottier, 2020). Victims of doxing do not just suffer from the immediate implications such as invasion of privacy and disclosure of sensitive and identifying information (e.g., addresses and social

[1] Lee (2022) refers to the stat of 'context collapse' when a content is posted onto a public social media platform by a social media user under their own profile, the user risk making themselves vulnerable by exposing themselves to an unknown audience who could interpret and recontextualise the original content in an infinite number of possible contexts.

security numbers) (Anderson & Wood, 2021; Douglas, 2016). The effects and implications of doxing can follow the victims for years on end, in some cases, hindering and limiting their ability to live their lives normally in both the real world and the online world (Anderson & Wood, 2021; Douglas, 2016).

Although doxing has become a widely known term and practice, the act itself carries a largely negative connotation amongst the wider populace as both the people and the law have begun to take the issue of privacy infringement and online safety more seriously (Anderson & Wood, 2021). More recently, Hong Kong had attempted to address this issue in the form of an amendment to the PDPO in the wake of the massive waves of doxing against law enforcement officers and many others during the 2019 protest movement (Cheung, 2021; Office of the Privacy Commisioner for Personal Data, 2022; Purbrick, 2019). Although some have argued this is a step in the right direction in addressing this ethically questionable practice where it could potentially have harmful consequences for the doxing targets, questions are also beginning to arise with regards to the underlying context and implications regarding issues such as freedom of speech, social justice, and the policing of cyberspace (Chang, 2020; Cheung, 2021; Chia, 2019).

Studies relevant to the legal dimension of doxing have focused more on the similarities to other cyber offences (Chang, 2020; Purbrick, 2019), rather than specifically examining any legislative text. Although Cheung (2021) discusses the legal implications of the legal measures introduced to address the issue of doxing in Hong Kong (hereinafter referred to as the 2021 Amendment), she did not examine the 2021 Amendment. Moreover, although there are studies which examines the consequential harms of doxing in general (Anderson & Wood, 2021; Douglas, 2016), studies which look at how consequential harms of doxing is being addressed legally, either through legislation, regulation or in front of the court of law, are scarce. Thus, the limited literatures on doxing, as well as the recent

legislation addressing this practice in Hong Kong, emphasise the need for a more encompassing study on the topic of doxing within the scope of law and its legal implications.

This research study aims to investigate and examine doxing and the effects it has in the context of Hong Kong, as well as to investigate and understand how doxing is legally addressed in the context of Hong Kong. To answer to these aims, three research questions are raised including 1) What are the challenges that doxing posed to law enforcement?; 2) How has doxing in Hong Kong been addressed by the 2021 Amendment?; and 3) What are law enforcement's response to doxing after legal measures were introduced to address doxing?

The content of this research study is divided into 6 chapters. This chapter – Chapter 1 – provided an overview of the general understanding of doxing, as well as provided the background and contextual basis of undertaking this research study, including the gap in the general literature on this subject. Chapter 2 provides a scoping literature review on the current academic studies and literature on the subject of doxing. Chapter 3 describes the methodology employed for this research study which is a qualitative case study to answer to the research aims and questions. Chapter 4 describes the findings of the research study in three sections, including doxing in Hong Kong before the 2021 Amendment, the legal measures introduced in the 2021 Amendment, and how Hong Kong law enforcement responded to doxing after the 2021 Amendment. Chapter 5 discusses the findings in chapter 4 in relation to the overall literature review in chapter 2. Lastly, chapter 6 provides an overall summarisation of the previous chapter, as well as identifying the limitations of this research study and potential topics which can be further address in future studies.

Chapter 2: Literature Review

1. Introduction

This chapter aims to explore the existing literature on doxing. The main objective of this chapter is to undertake an exploratory and scoping approach in reviewing the relevant literature and studies on the topic of doxing. As the majority of the studies specifically on the topic of doxing was conducted within the last decade, there are limited studies that are relevant for the purpose of this chapter. This chapter will also serve to provide context and basis for discussion in the discussion chapter of this research study. This chapter is divided into two sections. The first section discusses the literature on doxing being an extension of other cyber offences. The second section discusses the literature on doxing as being a unique phenomenon in the cyberspace.

2. Understanding doxing in academic literature

Studies specifically focusing on the topic of doxing are still at a relatively early stage, with many of the existing literature being a derivative or extension from discussions on other more well-known topics. Thus, contemporary discourses on this subject matter are fragmented, but some scholars have begun taking more interest in examining and studying doxing on its own merit and providing a clearer and deeper understanding into the nature of this practice. However, it would not be sufficiently comprehensive to discuss the literature on the topic of doxing without looking at the previous discourses that inform latter and more particular studies. This section provides an overview of the various aspects and approaches of the literature on doxing before delving into more specific studies.

2.1. Doxing as a variation of other cyber offenses

Although doxing has been around since the 1990s (Cheung, 2021), it has only become a subject of prevalence in academia within the last decade. Many of the existing studies on doxing examine this practice as an extension of other cyber offenses such as digital vigilantism, or technology-facilitated violence (TFV). Digital vigilantism, as the name suggests, refers to acts of justice seeking or punishment that occurs in response to perceived injustices which are expressed in the cyberspace (Loveluck, 2020; Trottier, 2020), whereas TFV refers to the harms or abuses which occur through the use of digital technologies (Bailey, et al., 2021). These two different approaches each provides a different perspective to examining doxing: the first examines the motives of doxing whereas the other focuses more on the consequential harms of doxing.

2.1.1. Doxing as a method of digital vigilantism

Doxing as an extension of digital vigilantism has been examined and studied by scholars, including Trottier (2020), Loveluck (2020), and Favarel-Garrigues et al. (2020). Despite having different aims and perspectives, the scholars of digital vigilantism all look at doxing as a method of carrying out digital vigilantism against a perceived injustice or wrongdoing, typically through utilizing an individual's personal details and information gathered from the internet to achieve their aims of justice or vengeance (Favarel-Garrigues, et al., 2020; Loveluck, 2020; Trottier, 2020). The literature on doxing through the lens of digital vigilantism frequently emphasise the intentions – often times the enactment of vigilante justice – of the doxers, whether through gathering and using the doxed information to bring humiliation and place social pressures on the doxing target as a form of punishment, or if the doxing is done as a means to bring public attention towards the doxing target, or to advance relevant public discourses (Favarel-Garrigues, et al., 2020; Loveluck, 2020; Trottier, 2020). The act of doxing here is typically done with the interest of the public in mind. For instance, the doxing of a child predator where

their personal data such as full name, current address and telephone number are publicised on the internet is done to bring the public's attention towards a perceived danger, which in this case is child predation.

On one hand, Trottier (2020) views doxing as a tactic to make an individual visible, through gathering and using a person's personal data against them, or as he phrases it, 'weaponizing' the different types of personal data of an individual to make them visible to the eyes of all audiences in the cyberspace. Consequently, this would render the doxing target visible to the reach and scrutiny of those audience, and hence, vulnerable to potential harassments from them (Trottier, 2020). Similarly, Favarel-Garrigues et al. (2020) also discuss doxing as the tactic or method of weaponizing an individual's visibility to serve the basic principle of digital vigilantism, mainly through publicizing the information and details that are gathered on the target of doxing and distributing them on public websites or web forums.

On the other hand, Loveluck (2020) is more specific, describes doxing as a tactic of a form or subset of digital vigilantism which he categorises as hounding. Hounding, as defined by Loveluck (2020), is one of four types of digital vigilantism which is characterised by the elements of investigating a specific target or event with punitive intentions through mass mobilization triggered by "intense outrage". Under this form of digital vigilantism, doxing is defined as the deliberate finding and publishing of specific personal data on an individual (e.g., address, phone number, etc.) that can potentially insult, humiliate, or threaten said individual. As the typology suggests, this can take the form of collective or group efforts, and the act or process of acquiring the information can be non-consensual or illegal.

2.1.2. Doxing as a form of technology-facilitated violence

Scholars such as Bailey et al. (2021) have studied doxing as a form of TFV, whereby the act of doxing is looked at more closely from the perspective of the harm it causes to the doxing target. As doxing is an online practice – enabled and enacted through the use of the internet to gather and search for another individual's personal data as well as to publish it – the harms and abuses resulting from a doxing act could have only occurred through the use of technology (Bailey, et al., 2021; Makinde, et al., 2021; Pacheco & Melhuish, 2021). The aspect of disclosing personal data without consent is viewed to be a cause of harm toward the doxing target by taking away the victim's ability to decide what personal data they are willing to share with others, and what data they do not want to share (Bailey, et al., 2021; Makinde, et al., 2021; Pacheco & Melhuish, 2021).

Bailey et al. (2021) raise that doxing can led the target to experience real world harms such as through physical stalking and harassments. The authors argue that through the disclosure of these data, not only did the doxer increase the likelihood of harms to the doxing target, but that such harms are very unlikely to have been reasonably foreseen (Bailey, et al., 2021). Thus, scholars of TFV perceive doxing as a form or subset of TFV since doxing and its consequential harms are only possible through the use of technology or a digital medium. The consequent harms in this case are emphasised as a point for discussion and more closely examined from the perspective of the doxed individual.

2.1.3. Alternate variant of doxing: China's Human Flesh Search

More interestingly, another approach within the literature on doxing is the examination and studying into a variation of this practice, otherwise, known as 'Human Flesh Search' (HFS). The practice of HFS, or otherwise known as 'internet crowdsourcing' (Huang, 2021), originated in the Greater China region, specifically within Mainland China, and it is a practice exclusive within the context of the cultures within the surrounding region (Baasanjav, et al., 2019; Gao & Stanyer,

2014). The HFS practice has been described and studied as a variation of doxing for its use of personal data disclosure to harm the intended target, specifically seeking to inflict shame through public ridicule or humiliation, or to hold the target accountable for their actions or inactions (Baasanjav, et al., 2019; e Silva, 2018; Gao & Stanyer, 2014; Han, 2018; Huang, 2021). Baasanjav et al. (2019) draw a comparison between HFS and doxing for their geographical and cultural distinction between China and other countries such as the U.S., respectively. The authors further argue that HFS within the context of China is used as a form of 'co-surveillance' practice by utilizing the populace of the cyberspace to enact an alternate form of social control where the government does not have to be the one directly enforcing the social values (Baasanjav, et al., 2019). In addition, they also suggest that this practice places constraints on the freedom of speech and expression of the wider public.

What differentiates HFS from doxing is not only its cultural context, but the distinction of HFS being an exclusively group or collective phenomenon that can be triggered not only by a perceived offense, but also for other miscellaneous reasons (Huang, 2021). In this sense, the practice of HFS can be seen as broader in nature compared to the general understanding of doxing. Huang (2021) gives an example that HFS can simply be triggered by the simple need to find out the identity of a beautiful individual from a picture in a social media post, lacking the element of intending to cause harm to that individual. Although this initial act might have been done in with harmless intentions, the data that are disclosed can potentially led to subsequent harms caused by malicious actors, such as through cyber stalking (Huang, 2021). Gao and Stanyer (2014) also lists out 12 cases of socially and morally motivated cases of HFS – more akin to acts of doxing with the purpose of digital vigilantism as discussed above. Most of these cases describes the Chinese netizens' effort of identifying wrongdoers which have committed a socially or

morally unacceptable acts in line with the Chinese culture and norms, for instance, infidelity, insulting the Chinese culture, and animal abuser.

However, it should be noted that within the context of the Chinese practice, HFS practice also presents a dimension which specifically focuses on a kind of doxing effort that targets corrupted politicians or government officials as a method of holding them accountable for their actions (Baasanjav, et al., 2019; Gao & Stanyer, 2014). Goa and Stanyer (2014) also present 8 cases of HFS cases which specifically target toward politicians and government officials. The authors note that the nature of how these cases were conducted – from fact checking government announcements to identifying corrupted politicians and government officials – is a reflection of how the Chinese netizens respond to and interact with the Chinese government (Gao & Stanyer, 2014).

2.2. Doxing as a unique practice in the cyberspace

All these approaches discussed above predominantly frame the studies on doxing within an area of interdisciplinary studies which overlaps both social and behavioural studies with studies of technology and digital media. Each of the approaches offers a different perspective and each highlights a different dimension to the practice. More recently, researchers have elected to examine and study doxing as a unique practice on its own merit instead of an extension of other offenses. In addition to the qualitative studies, quantitative studies have also begun to emerge to provide a more in-depth insight into this practice.

On one hand, scholars such as Anderson and Woods (2021) have built on the conceptual study of doxing by David M. Douglas (2016), who was the first to extensively examine doxing and identify different categories of doxing by looking at the consequential harms of the practice. On the other hand, scholars such as Chen et al. (2019) and Snyder et al. (2017) have chosen to further examine the forms,

intentions, and characteristics of doxing by undertaking empirical studies to provide further evidence-based insights on doxing. Being a social phenomenon, there are also scholars who have approached the ethical and moral aspects of doxing, while also building on Douglas's work which argues for exceptional circumstances where doxing maybe justified (Barry, 2022; Gonella & Nericcio, 2017). There are few studies that have touched upon the legal perspective on the doxing practice (Cheung, 2021; MacAllister, 2017). However, there are also studies that take a well-rounded approach in examining doxing, including the forms, characteristics and challenges it presents (Anguita, 2021).

2.2.1. Categorizing the type of doxing

Douglas (2016), in his conceptual analysis of doxing, proposes three types of categories for doxing: 1) deanonymizing doxing, 2) targeting doxing, and 3) delegitimizing doxing. He rationalises this categorization based upon the type loss the doxing targets experienced, and defines each category by the type of information that is disclosed through the act of doxing (Douglas, 2016). Douglas posits this categorization on the values of anonymity and obscurity. He states that the act of doxing would undermine the veil of security and protection afforded by being unknown and inaccessible to the general others (Douglas, 2016). Control of information disclosure is also an important aspect of Douglas's rationalization for the values that would be lost through doxing. If a person is doxed, they would no longer be able to decide which personal and private information they can share and make public (Douglas, 2016).

Deanonymizing doxing refers to the type of doxing which covers the disclosure of all types of identifiable information, notwithstanding whether or not the information was available to the public prior to the doxing event (Douglas, 2016). Although this type of doxing covers the widest range of the types of information being disclosed, the type of loss suffered by the doxing target maybe relatively

insignificant, which is the loss of anonymity (Douglas, 2016). For some doxing targets, this loss entails nothing more than an inconvenience over the loss of choice on which information they wish to share, or perhaps would not have even been perceived as a harm at all.

Targeting doxing refers to the type of doxing by which the information being disclosed is specific or detailed in nature, which can allow the doxing target to be linked to their real identity and be physically located in the real world (Douglas, 2016). This type of narrowed down information (e.g., home address, place of work, place of study, etc.) entails the loss of obscurity and privacy for the doxing target (Douglas, 2016). This means that the information being disclosed creates a channel of access to the doxing target; hence, opening the possibility for potential harms to occur to them in the real world. Although the data being disclosed can be very minute or specific, the harms experienced by the target of this category of doxing can vary greatly from simply being a harmless annoyance (e.g., spam mails being sent regularly to the subject's real world home address, prank telephone calls, unwanted subscriptions mailed to home address, etc.) to severe potential real-world harms or injuries (e.g., real-world stalking, mailing dangerous items to the target of doxing, harassment campaigns in the real world, etc.) (Douglas, 2016). This category of doxing is often used by malicious actors who utilise doxing as a tool with the intention to harass, harm, or cause other types of injuries to the target of the doxing acts (Douglas, 2016). Due it being frequently used to conduct malicious acts, targeting doxing is the category of doxing to be most frequently reported and elicit responses from law enforcements (Douglas, 2016). Thus, targeting doxing can be understood as a more narrowed, or intentionally motivated act used to serve the interests or objectives of the doxers.

The third category of doxing described within Douglas's typology is delegitimizing doxing which refers to the type of doxing by which the information being disclosed

is a type of personal and private information that has the potential to vilify, undermine, or destroy the credibility of the doxing target (Douglas, 2016). Through the acts of delegitimizing doxing, the target of doxing experiences a loss of credibility, by which the harms suffered by the target can range from moderate (e.g., loss of reputation among peers, loss of professional credibility, or loss of trustworthiness within his/her communities, etc.) to severe (e.g., loss of employment, psychological and/or physical traumas or injuries, harassments or attacks in the real world, etc.) (Douglas, 2016). This category of doxing is the most widely recognised because it is often utilised as a tool to coerce targeted subjects in to conforming with the norms or the opinions, beliefs, and standards of the majority, in addition to serving as a tool to remove or diminish the credibility of important figures within their communities, whether the doxing target deserves these negative responses or not (Douglas, 2016). In this manner, delegitimizing doxing can also serve as a check-and-balance tool, as well as a tool for the majority to scrutinise and hold public or important figures within their communities accountable for any wrongdoing.

Anderson and Wood (2021) further develop on Douglas's typology of doxing by introducing a fourth category in addition to the three described above: disadvantaging doxing. They rationalise the need for this fourth dimension due to the fact that Douglas's definition only covers the release and disclosure of an individual's personal data, and highlight the fact that a corporate entity can also be a target for doxing (Anderson & Wood, 2021). Disadvantaging doxing refers to the disclosure of proprietary information, rather than personal data, of a corporation which results in the loss of competitiveness and economic advantages against other corporations (Anderson & Wood, 2021). Anderson and Wood further distinguish this category of doxing by highlighting that corporate or organization can be the target of both disadvantaging doxing and delegitimizing doxing. A corporation or

organization can suffer the loss of competitive edge or come under public scrutiny and subsequent boycotting due to the release of proprietary information, as well as the loss of credibility due to the nature of specific private information being disclosed regarding its officers (Anderson & Wood, 2021). This is a crucial addition to the overall typology of doxing as it expands upon the scope of doxing target and introduce a new element of harm and loss which can result as from doxing.

In addition to the four categories of doxing, Anguita (2021) also present another mode of characterizing doxing by differentiating the variations of this practice as being positive and negative. The positive category of doxing covers a range of activities by many different types of actors. Institutions and law enforcement agencies practice this category doxing on a regular basis such as through conducting background checks for investigation and hiring purposes (Anguita, 2021). Customers who are dissatisfied with a product or service provider also participate in this positive category of doxing through disclosing information on poor products or services (Anguita, 2021). In some instances, such as with the practice of HFS, the general public are the ones to carry out acts of positive doxing to achieve social justice or serve a common public interest of punishing wrongdoers or hold a public figure accountable (Anguita, 2021). These activities are viewed as positive doxing as the information gathered are for illegitimate and legal purposes, and if the information is disclosed, it is to serve a common public interest.

The negative category of doxing covers activities which are more commonly associated with what is typically perceived of the doxing practice. The objective of doxing under this category is typically to cause some form of harm, whether physical, psychological or otherwise, to the doxing target (Anguita, 2021). The specific motives driving negative doxing vary from case to case, but doxers usually attempts to illicit a negative response towards the doxing target (Anguita, 2021). Doxing an individual through revealing any information that can be used to identify

them in the real world is a form of negative doxing (Anguita, 2021). Although the initial motives may not have been malicious, the subsequent uses of the disclosed information to potentially harm of the doxing target can result in detrimental consequences. Public figures who more openly express their political or moral opinions are more likely to be at the receiving end of negative doxing, as their opinions would more often than not illicit negative response from those who do not share the same perspective (Anguita, 2021).

2.2.2. Empirical studies on doxing

Snyder et al. (2017) conducted the first quantitative study on doxing with the purpose of providing more empirical insights into this practice. This study demonstrates the prevalence of doxing on online social network platforms, who are the relevant parties involves, inferring the intentions of the doxers, and the effects doxing in the communities involved. In their study, Snyder et al (2017) designed and deployed an automated doxing-detection tool that is able to identify doxing files on well-known doxing websites. From the data gathered, they were then able to analyse the frequency of doxing, the contents of the doxed materials, the targets of doxing, and the effect of doxing on social network platforms (Snyder, et al., 2017). The study identifies the demographic information of the doxing targets as being predominantly males between the age range of 10 to 74 (Snyder, et al., 2017). The study also identifies the communities where doxing mostly occurred. The majority of identified doxing materials are associated with the gamer community, followed by the hackers and celebrities (Snyder, et al., 2017).

In addition to identifying the demographic of relevant parties associated with doxing, four motives could be inferred from the doxed materials including justice for a third party, revenge against harms done, competing to show their abilities, and in support or against a political standing (Snyder, et al., 2017). Six social network platforms are identified as being the most frequent platform to carry out acts of

doxing including Facebook, Google+, Twitter, Instagram, YouTube, and Twitch, with Facebook accounts being associated with the most doxed materials (Snyder, et al., 2017). Accounts associated with doxing were found to have increased in closure and privacy following instances of doxing, which in turn, creates additional harms to the doxing targets through increased social isolation (Snyder, et al., 2017). It is also found that social network platforms that have deployed abuse filters such as Facebook and Instagram, are able to offer more protections to their users against harms resulting from doxing (Snyder, et al., 2017).

Another empirical study is conducted by Chen et al. (2019) with the purpose of looking at adolescent's participating in the doxing practice in Hong Kong. The authors view doxing as technically unsophisticated which allowed more easier barrier of entry to participate for the younger population at a time when information sharing has become a trend among adolescents (Chen, et al., 2019). Among the sample population of secondary school students, the study found that there is a one to ten ratio of students that had engaged in doxing, and those who had been the doxing target were subsequently more likely to commit acts of doxing themselves (Chen, et al., 2019). Moreover, those who had their personal data disclosed had previous experiences in relation to doxing, such as being doxed, a bystander, or having doxed others (Chen, et al., 2019). The study also finds that social doxing is more likely to commit by female students to obtain social information such image and relationship status, while hostile doxing is more likely to commit by male students to obtain personal identifying and living situation information that has the potential to cause harms such as harassment and attack (Chen, et al., 2019).

2.2.3. Ethics and morality of doxing

Gonella and Nericcio (2017) discuss the dimension of morality of doxing, and offer two theoretical perspectives on the moral implications of this practice. The study offers an examination of the different moral perspectives on doxing. The first moral

theory that the authors discuss revolves around the theory of consequentialism which posits that the morality is determined by comparing the beneficial and detrimental consequences of an action (Gonella & Nericcio, 2017). Through acts of doxing for revenge or social justice, answering to an act that already causes harms by causing more harms only results in more net harms done creating happiness or satisfaction that can be derived from the act of doxing (Gonella & Nericcio, 2017). The second moral theory that the authors discuss the theory of deontology which posits that disregarding or violating one's own duties and obligations is morally wrong, even if it means creating undesirable consequences for others (Gonella & Nericcio, 2017). From the view of a deontologist, the act of doxing and the act that illicit the response of doxing are both morally incorrect, especially in the cases of revenge or social justice doxing. A person who commits a deviant act would have breached a moral or social obligation for it to illicit a negative response in the form of doxing. Conversely, a person who commits the act of doxing in response to that deviant act would have breached a universal moral or social obligation of not causing harms to others.

In his study on the ethics of doxing sexual transgressors, Barry (2022) posits that doxing can be justifiable and is akin to enforcing legal rules against wrongdoers. The author lays out three bases for doxing. First, the author argues that doxing can be morally justifiable as an act of warning. Doxing can be used a more swifter warning mechanism to disseminate information to the public of wrongdoers, so the public can be aware and take pre-cautionary measures to avoid harms, not unlike law enforcement posting public notices (Barry, 2022). Although doxing to warn the public may sometimes implicate an innocent party, the author argues that the risks can be tolerated if it ultimately serves the common interests of the public (Barry, 2022). Second, the author argues that doxing can be a morally acceptable act of punishment. The author argues that if a person commits a wrongdoing that causes

harms, then that person has, through their action of harming others, forfeited the right to not be harmed by others (Barry, 2022). In this case, a retributory doxing that causes equivalent harm should be morally justifiable as a form of punishment towards the doxing target. Third, the author argues for that doxing can be a morally justifiable act based on public reasons, or reasons which most the general public would likely agree with (Barry, 2022). The author argues that the existence of moral and social norms, and the breach of these norms would illicit a morally acceptable response, such as through doxing, to correct or redress this non-conformity (Barry, 2022).

2.2.4. The legal dimension of doxing

Arguments have been raised with regards to the justification of doxing before the court of law. Douglas (2016) bases his argument for the justification of doxing on the concept of public interest. The act of doxing is justifiable so as long as it is conducted with a legitimate interest of the public as the rationale or motivation. Douglas (2016) argues that doxing is acceptable if the rationale behind revealing the identity of the target is a compelling justification for the interest of the public. He also notes that the information disclose is only acceptable to the extent which it can sufficiently serve as evidence to establish wrongdoing, and the burden of proof will fall to the person who intend to disclose such information (Douglas, 2016).

This public interest justification is expanded upon by Cheung (2021) who further expands upon Douglas's rationale by arguing that this legal defense should be applicable to doxing within the scope of establishing accountability for public officers where there is a reasonable basis linking the target of the doxing to an alleged wrongdoing. However, she notes that such cases should only be applicable to those entrusted with the responsibilities of governing and safeguarding the interests of the public, and highlights that although there are specifications on the types of information which are restricted from being disclosed in legislation

applicable to cases of doxing, there has yet to be any law specifying the use of public interest as a legal defense in cases of doxing (Cheung, 2021).

Demonstrating the legal elements and thresholds pertaining to doxing in the court of law can also be very difficult as, in most states and countries, there are no specific legislation with regards to the recourses for grievances that are the result or consequence of doxing, with the closest adjacent being cyberstalking or cyber-harassment (MacAllister, 2017). In these adjacent offences, the elements to be proven typically includes the intent of the perpetrator in committing the act, as well as establishing the harms the are the result of these acts (MacAllister, 2017). Moreover, under offences such as cyber harassment, a perpetrator can be found guilty of a criminal offence (MacAllister, 2017). In this regard, MacAllister posits that doxing comprises of enough similar characteristics to warrant the same legal treatments, given the harms that it can cause.

Victims of doxing generally have very little to no recourse options available, or are shamed into not seeking help or assistance from law enforcement, leaving this practice to grow and expand with little to no moderation or policing (Anderson & Wood, 2021; MacAllister, 2017; Trottier, 2020). For instance, the criminal prosecution of cases of doxing within the US are contingent on the outcomes or consequences of the doxing act itself rather than the breach of privacy that the target experienced due to the initial disclosure or publication of information (Anderson & Wood, 2021). Similarly, cases in which doxing have been brought to court under claims of torts face difficulties in fulfilling the elements to win claims for remedies as the definition of applicable vocabularies used in these cases (e.g., private information) are often times out of date; hence, inapplicable to the online context (MacAllister, 2017).

3. Conclusion

In summary, this chapter presented an overview on the literature on doxing, including the different approaches taken by scholars in examining and studying doxing. The first section discussed the literature approach on doxing being an extension practice of other cyber offences. This included the literature on doxing as a form of digital vigilantism, doxing as a form of TFV, and doxing a variant of HFS. The second section discussed the literature approach on doxing being a unique practice in the cyberspace. This included the literature on the categories of doxing, the empirical studies on doxing, the ethics and morality of doxing, and the legal dimension of doxing.

Chapter 3: Methodology

1. Introduction

This chapter describes the methodology for this research study. This research study has two aims which are to investigate and examine doxing and the effects it has in the context of Hong Kong, as well as to investigate and understand how doxing is legally addressed in the context of Hong Kong. To answer to these aims, this research study raises three research questions: 1) What are the challenges that doxing posed to law enforcement?; 2) How has doxing in Hong Kong been addressed by the 2021 Amendment?; and 3) What are law enforcement's response to doxing after legal measures were introduced to address doxing?

This chapter is divided into two sections: the research approach and research method. The research approach covers aspects such as the philosophical worldview, the research design, and the research methods. The research method section covers data collection and recording, and data analysis and interpretation. Lastly, the content of this chapter is summarised in a concluding summary section.

2. Research approach

To answer to the aims and objectives of this research study, a research approach is needed to provide a clear roadmap as to how the research study will be conducted. A research approach refers to the plan and procedure for studying the research topic which encompasses various aspects and decisions, including the broad philosophical assumption and the detailed methods used to carrying out the study (Creswell & Creswell, 2018). There are three general approaches to conducting a research study: 1) qualitative approach; 2) quantitative approach; and 3) mixed method approach (ibid). There are three main components that inform the decision as to which research approach is appropriate for a study, including 1) the philosophical worldview; 2) the research design; and 3) the research method (ibid).

Taking the aforementioned components into consideration, this research study adopted a qualitative research approach for a few reasons. First, a qualitative research approach is suitable in addressing a social problem. As the topic of this research study concerns a social practice and its implications within the sphere of social science, it would be more appropriate to select a research study approach which allows for the interpretative understanding of a social issue. Second, as the topic of this research study concerns the exploration and examination of legislative texts and secondary data, it would be more appropriate to select a research approach that allows for interpretive analysis of text-based data. Third, since the research questions raised within the research study are context-specific, it would be more appropriate to select a research approach which allows larger themes to emerge from the particulars and details to identify the challenges. Fourth, a quantitative research design is not useful or helpful in answering to the aims and research questions of this research study, as it rooted in statistical and numerical analysis of data to prove a pre-established theory (Creswell & Creswell, 2018). In other words, a quantitative research design is used for testing a measuring quantifiable data which is not the objective and aim of this research study. A mix method research design is also unsuitable for the purpose of this research study. The mix method research design derives selected elements from both qualitative research design and quantitative research design, the latter of which is suitable and unnecessary for the purpose of this research study (ibid).

The following sections describe the philosophical worldview, the research design, and the research method that informed the approach of this research study.

2.1. Philosophical worldview

This research study was approached from a constructivist worldview as this research study attempts to construct meaning from the subjective interpretation of the subject matter. The researcher's philosophical worldview mainly fits under the

constructivist philosophical worldview, based largely upon previous academic discipline that is posited in social and legal studies, which also aligned with the assumptions of the constructivist worldview for a few reasons. Constructivist takes on the assumption that meanings are subjectively generated and interpreted by humans as they socially interact with world around them (Creswell & Creswell, 2018; Creswell & Poth, 2018). Moreover, it posits that the way humans interpret meanings from their surrounding is context-based and is influenced by the individual's personal background and experiences (ibid). In other words, the meanings generated is derived from a social context, which align with the researcher's background in social studies, as well as contribute to the understanding of the social and legal underpinnings of the nature of this study.

2.2. Research design

Before identifying the research design, it is useful to identify the reasoning or interpretive approach used within this research study. This research study would greatly benefit from an inductive reasoning approach. An inductive reasoning approach aims to explore rather than test and prove a theory such as with a deductive reasoning approach (Creswell & Creswell, 2018). It is commonly employed when there is limited literature on a certain subject and there are no established theories to be tested, or when the goal is to explore and discover new elements regarding the subject (ibid). This is an appropriate reasoning approach in answering to the aims and research questions of this research study which is to investigate and better understand doxing with an added emphasis of examining the legal implications of this social practice. A deductive reasoning approach is unsuitable for this research study as the aim of this approach is to test and prove or disprove a theory (ibid). Without an existing theory to be tested, which differs from the objectives and aims of this study, then a deductive reasoning approach cannot be undertaken.

This research study adopted a case study research design for a few reasons. First, the case study design is a research design that is primarily employed within the field of qualitative research to explore a clear and identifiable case (Creswell & Creswell, 2018; Creswell & Poth, 2018; Zainal, 2007). This research design allows for an in-depth examination of data or materials within a research study by exploring and investigating one or more events concerning a specific phenomenon by contextually analysing them (Zainal, 2007). Second, the case study design is also able to allow the researcher to investigate and gain an in-depth understanding of the subject of the case or cases, especially within the disciplines of psychology, law, political science, and medicine (Creswell & Poth, 2018). In the case of this research study, it would allow for an in-depth understanding of the legal perspective on doxing and how it is being addressed in the legislation, as well as the challenges faced in regulating a social and cyber practice such as doxing.

After selecting the case study as the research design, it is also important to consider and determine the intent and type of case study to be conducted for this research study, which would also inform the research method as well. The case study design is categorised by the objective of the research study or the interest of the research study (Zainal, 2007). Zainal (2007) identifies 3 types of case study method: intrinsic case study whereby the selected case is explored and examined on its own merit; instrumental case study whereby a group of selected cases are examined to observe behavioral patterns; and collective case study whereby data are collected and compiled from multiple different sources. This research study adopted an intrinsic case study design to answer to the aims and the research questions of this research study which is exploratory in nature and focuses on the case itself within its own unique context and surrounding.

2.3. Research method

Within each of the three research approaches described above, there are different research methods which are specific to each approach (Creswell & Creswell, 2018). The research method is the detailed procedures of conducting the research study, and consists of the forms and procedures of data collections, data recording, data analysis, and data interpretation (ibid). Each part of this process is not distinct and separate from one another; they are interrelated (ibid).

2.3.1. Data collection and recording

The data collection process includes determining the intent of the type of data to be collected for the research study, the boundaries of what to be included in the research study, the means and materials to be collected, and the protocol for recording the data collected (Creswell & Creswell, 2018). As this research study adopts a qualitative research approach with a case study research design, it was most appropriate to tailor and refine the research method based on the considerations of the qualitative research approach.

The boundaries set for the data collection process are broad to allow the best outcome from this exploratory study. The data used for the purpose of this research were gathered only from public and government archives, specifically from the online database of the HKPCPD. These include the three versions of the legislative texts of the PDPO, the annual reports of the HKPCPD, documents such as surveys that were published on the database, media records and statements from the HKPCPD.

Third, as this research study aims to explore how doxing is addressed in the Hong Kong amended legislation, the types of data that were primarily collected and utilised for the purpose of this research study were primarily secondary data in the form of qualitative documents. Qualitative documents refer to public documents, official reports, newspapers, legal archives, legal opinions, published records, etc.

(Creswell & Creswell, 2018). Secondary data refers to any data which is not obtained first-handed and has been collected, compiled, or archived, and is now being utilised to serve a different purpose that what it was originally collected for (Silva Martins, et al., 2018). This research study also utilised secondary data gathered only from public and government archives, specifically from the online database of the HKPCPD. These include the three versions of the legislative texts of the PDPO (Personal Data (Privacy) Ordinance (Cap. 486), 1996; Personal Data (Privacy) Ordinance (Cap.486), 2012; Personal Data (Privacy) Ordinance (Cap. 486), 2021), the annual reports of the HKPCPD (HKPCPD, 2020; HKPCPD, 2021; HKPCPD, 2022), documents such as survey that was published on the database (HKPCPD, 2021), and other relevant publications and records from the HKPCPD.

Next, after the data have been collected, they were categorised and sorted in separate sheets within the Microsoft Excel (ME) program. Within each ME sheet, each piece of data was given a referencing number (e.g., 001, 002, 003), a label describing the specific type of data (e.g., data, text), a brief summary of the data piece itself (e.g., HKPCPD's response after 2021 Amendment), a list of key points from the data piece, and a label of the relevant research questions which the data piece answers to (e.g., Objective 1, Objective 2, Objective 3). This sorting protocol has the advantage of streamlining the referencing process by allowing the researcher to go back and forth between different data and observe any emerging patterns and themes. Not only was this very useful in organizing the overall findings into a cohesive narrative that also answers towards the research questions raised, it also allowed general themes and sub-themes to be observed as well.

2.3.2. Data analysis and interpretation

After the data have been collected and recorded, the next step was to analyse, interpret and present the data as findings. The data that have been collected and recorded were analysed using the thematic analysis approach. Thematic analysis

approach is a process of qualitative data analysis which can be employed in various different paradigms of research (Kiger & Varpio, 2020), including within the constructivist paradigm in which this research study was approached from. It is utilised as a method for describing and analyzing data, which involves the process of coding and constructing themes (ibid), and was used within this research study to identify patterns, common or reoccurring themes which answered to each of the objectives, as well as more specific sub-themes that emerged within the greater themes. This method of data analysis is appropriate when used to explore, and understand, investigate and examine unique events, experiences, and phenomena (ibid). This is beneficial in answering to the aims and research questions of the research study.

There are various guidelines on how to procedurally conduct a thematic analysis, but this research study adopted the design of Clark and Braun which lays out six sequential steps for analysis a data set thematically (Clarke & Braun, 2017). The first step is to become familiarise with the chosen data set, or data familiarization, by systemically and repeatedly going through all the data collected to allow the researcher to become familiar with the contents as well as improving the researcher's ability to recognise similar or recurring ideas as they go back and forth through different data (ibid). After the researcher has gotten to known the contents of the data set well enough, they could then procced to organise data points into relevant themes by taking notes of various repeated and recurring ideas or concepts through coding them into different theme which would later become points for discussion (ibid). Third, the researcher now needs to identify the relevant emerging information points and then sorting the information points into relevant themes (ibid). The next step is to review the themes as well as the information points sorted under each theme to ensure that each of them fits into their respective theme coherently and concisely to answer to the research question and meet the research

aim and objectives of this research study (ibid). Next after reviewing the themes, the researcher then provides definitions and names for each theme and outlining its importance in answering the research questions (ibid).

For this research study, all the steps described above were conducted simultaneously as the data were being collected and recorded, through the mechanism of labelling the data in accordance with each of the research question they answered to. On top of the three general themes that answer to each of the three research questions, some data were also additionally coded as "context". Thus, the data were coded in accordance with the following themes: 1) context of legislation; 2) doxing in Hong Kong before the amendment in 2021; 3) changes made to the legislation in the 2021 amendment; 4) law enforcement's response to doxing in Hong Kong after the amendment in 2021.

As the last step, the researcher then constructed and reported upon the findings of the research study in a chronological narrative. The research findings are arranged into three sections: doxing in Hong Kong prior to the 2021 amendment, what changes were made in the 2021 amendment, and law enforcement's response to doxing after the 2021 amendment. Then, these research findings are discussed and presented the interpretation of the findings by referencing back to other literatures to strengthen the contexts and analysis of the presented findings. This last step is sectioned into a separate discussion chapter which follows the research findings chapter.

3. Conclusion

In summary, this methodology chapter describes the research design and methodology choices for this research study and the reasonings which informed these choices. The chapter first provides an introductory section which reiterates the aims and research questions of this research study, as well as describes the

outline of this chapter. Next, this chapter provides the details of the research methodology for this research study which includes two sections. The first section of research approach describes in details the three choices which informed the decision to select the qualitative research approach for this research study: the philosophical worldview, the research design, and the research method. This research study adopts a constructivist philosophical worldview, an intrinsic case study research design, and qualitative-based research methods. The details regarding the research method are divided into data collection and recording, and data analysis and interpretation. The second section of the research approach describes other aspects of consideration which also influenced the decision on the research approach. The aspects discussed are the nature of the research problem, the researcher's personal background and experiences, as well as the targeted audience of this research study. Lastly, this chapter concludes by recapping the key aspects of the chapter.

Chapter 4: Research Findings

1. Introduction

This chapter describes the findings of this research study that aims to investigate and examine doxing and the effects it has in the context of Hong Kong, as well as to investigate and understand how doxing is legally addressed in the context of Hong Kong. The findings of this research study are divided into three sections and presented in a chronological narrative. The first section presents the relevant key findings on doxing in Hong Kong in the period leading up to the 2021 Amendment. The second section presents the relevant key findings concerning the changes introduced in the 2021 Amendment. The third section presents the relevant key findings regarding doxing in Hong Kong after the 2021 Amendment came into effect. The chapter concludes with a summary of the relevant key findings presented in the three sections.

2. Research Findings

This research study presents its finding of the case study in three sections. The first section explores and examines doxing in Hong Kong before the 2021 Amendment came into effect and the challenges that doxing posed. It also examines the background of the PDPO which is the base legislation for the changes made in the 2021 Amendment. The second section explores and examines the three changes introduced in the 2021 Amendment. The third section explore and examines doxing in Hong Kong and the HKPCPD's response after the 2021 Amendment came into effect.

2.1. Doxing in Hong Kong before the 2021 Amendment

The first doxing case was reported to the HKPCPD on 14 June 2019 during the beginning of the 2019 Hong Kong protest movement. From this period onward,

doxing cases reported in Hong Kong spiked to an unprecedented number during the period of the protest movement. Along with the increased in number of doxing cases, new concerns and challenges have also emerged. This has also led to garnered supports to bring legal changes to address these concerns and challenges under the legislative umbrella of the PDPO.

2.1.1. Challenges posed by doxing in Hong Kong

With the context of the 2019 protest movement in Hong Kong, the HKPPD has recorded and reported a large number of doxing cases between 2019 and 2021. This increase is most notable between mid-2019 and mid-2020 whereby the HKPPD received and handled 4,707 doxing cases out of a total of 11,220 complaint cases. In addition to the 4,707 doxing cases received and handled by the HKPCPD between the period of mid-2019 and mid-2020, there were 2,665 separate doxing cases specifically related to the doxing of law enforcement officers and their family members. Combined together, the total number of doxing cases during this period amounted to 7,372 cases, more than a third of which revolved around police officers and their family members.

The number of doxing cases reported decreased by approximately 80% during the next year in the period between mid-2020 and mid-2021 whereby the HKPPD received and handled 957 doxing cases out of a total of 3,157 complaint cases. This is an approximately 71% decrease from the number of doxing cases in the year prior period. Unlike the previous year period, there is no specifications as to how many of these cases revolve around police officers and their family members.

In the period between mid-2019 to mid-2021, the HKPPD received and handled a total of 5,664 doxing cases out of a total of 14,377 complaint cases combined. It is observed that the majority of the doxing cases that were reported in this two-years period is situated in the period between mid-2019 and mid-2020. This is roughly

the timeframe during the height and right after the 2019 protest movement where social unrest was at an all-time high in Hong Kong.

Although the protest efforts were slowly tapering off in the early to mid-2020, there were still some lingering effects and moments of unrest among the general populace. Before the introduction of the 2021 Amendment, the HKPPD had to handle and intervene with doxing cases on an ad hoc basis. During this period of time, the HKPPD was mildly successful with their intervention attempts. During the period between mid-2019 to mid-2020, the HKPPD had contacted online platforms 166 times with the requests to remove a total of 2,867 web links related to doxing. Out of the 2,867 requests to remove these web links, only 1,777 web links were eventually removed, which amounts to a success rate of approximately 62%. The HKPPD had seen more success in this endeavor during the period between mid-2020 to mid-2021 whereby there were 3,912 web links related to doxing that were removed, bringing the total of number of removed web links related to doxing to 5,689 web links.

With the high number of cases, breach of data and privacy has become an issue of concerns not only among Hong Kong law enforcement, but also among the general public in Hong Kong as well. In a 2020 survey by the HKPPD, 36% out of 1,024 respondents reported that they had experienced misuse of their own personal data. Only 11% of the respondents who had experienced misuse of their own personal data officially lodged a complaint. For those who had had not officially lodged a complaint, the major reasons that were provided include: 1) 35% did not know where to lodge a complaint; 2) 21% perceived the process of lodging a complaint as too troublesome; and 3) 21% perceived the issue they had experienced to be not important enough to spend time on.

In addition to the Hong Kong public's negative experiences with misuse of personal data, the survey found that a majority of the respondents was also strongly

supportive of bringing legislative changes to address issues of doxing. Among all of the surveyed participants, 44% was fully in support of giving the HKPCPD the powers to remove doxed information from the internet, 42% was fully in support of giving the HKPPD the powers to conduct criminal investigation regarding doxing cases, and 39% was fully in support of giving the HKPPD the powers to prosecute doxing cases.

2.1.2. The Personal Data (Privacy) Ordinance

The PDPO is a data protection and privacy law in the jurisdiction of Hong Kong which came into effect in December 1996. It is implemented by the HKPCPD which is an agency that is independent from other government bodies with the purpose of monitoring, supervising, promoting and enforcing compliance with the PDPO to protect the individual's privacy with regards to their personal data. The purpose of the PDPO is to ensure there is adequate data protection within the Hong Kong jurisdiction and comply with international treaties regarding human rights obligations.

There have been two major amendments made to the PDPO since it initially came into effect in 1996. The major first amendment came into effect in 2012 which introduced new sections on direct marketing and additional sections on data protection. This occurred as a response to emerging privacy challenges and growing public concerns regarding these challenges, especially with regards to the use of personal data in direct marketing. The second major amendment came into effect in 2021 which introduced legal changes to address doxing in relation to the use of personal data. This latest amendment aims to combat the increasing number of doxing cases which poses a challenge to the privacy of Hong Kong citizens and raises concerns among its citizens regarding public safety.

2.2. Analysis of the 2021 Amendment

As a response to the increasing number of doxing cases as well as the growing public concerns and challenges presented, an amendment was made to the PDPO, known as the 2021 Amendment, which came into effect on 8 October 2021. The 2021 Amendment aims to combat doxing through. Although the 2021 Amendment does not specifically use the term “dox”, “doxing”, or “doxxing”, the offences introduced in the amended sections ascribe to the characterizing elements of doxing in academic literature, as well as being described and referred to as doxing offences by the HKPPD in official statements and documents.

In a media statement, the HKPPD states that the 2021 Amendment is introduced to serve three objectives as a response to the increasing number of doxing cases in Hong Kong. First, the 2021 Amendment introduces a two-tier system which criminalised doxing. Second, the 2021 Amendment empowers the HKPPD to investigate and prosecute doxing cases and other related offences. Third, the 2021 Amendment confers statutory powers to the HKPPD to issue cessation notices to remove doxed information.

2.2.1. Criminalising doxing as an offence – The two-tier system

The 2021 Amendment introduces section 64 with the purpose of criminalising doxing. Under section 64, a two-tier system of doxing offence is established which introduces two levels of severity of doxing offence. First, section 64(A) addresses a summary doxing offence which is a minor or lesser offence which is usually decided in court without a jury and carries a lesser term of punishment. Second, section 64(3C) addresses an indictable doxing offence which is an indictable offence is a serious offence which is usually decided in court with a jury and carries a heavier term of punishment.

Under section 64(3A), the first tier of summary offence addressing doxing is as follows:

> A person commits an offence if the person discloses any personal data of a data subject without the relevant consent of the data subject—
>
> (a) with an intent to cause any specified harm to the data subject or any family member of the data subject; or
>
> (b) being reckless as to whether any specified harm would be, or would likely be, caused to the data subject or any family member of the data subject.

This description of the summary offence above presents three thresholds to satisfy in order for an act to be considered as an offence: non-consensual disclosure, intent to cause harm, and being likely to cause harm. First, the act of disclosing personal data is done without the relevant consent of the data subject. The 2021 Amendment provides clarification on the term "relevant consent" as referring to the consent given by the data subject or on behalf of the data subject. The consent needs to be expressly given, and has not been expressly withdrawn through a written notice of consent withdrawal.

Second, the non-consensual disclosure is done with the intent to cause specified harm to the data subject or any of their family member. Under this section, intent to cause specified harm needs to be proven to demonstrated that the suspect has the mental state to cause harm in carrying out the disclosure of data. The 2021 Amendment provides clarification on the term "family member" as referring to a person who is related to another person by blood, marriage, adoption or affinity. The 2021 Amendment also provides clarification on the term "specified harm" which includes: "(a) harassment, molestation, pestering, threat or intimidation to the person; (b) bodily harm or psychological harm to the person; (c) harm causing the person reasonably to be concerned for the person's safety or well-being; or (d) damage to the property of the person." The scope of specified harm is dependent

on the relevant facts and circumstances of each case, including but not limited to the content concerned, means of expression, context of the content, how the content is being distributed, the extent of the distribution, the veracity of the content, characters of the data subject or their family members.

Third, the non-consensual disclosure act is done recklessly as to likely cause harm to the data subject or any of their family member. Recklessness is needed to demonstrate that the suspect had committed the act with a set intention to cause harm, and that it was not done out of negligence. Determining and interpreting if a reckless act by a suspect is likely to cause specified harm to a data subject or any of their family member would be left to the discretion of the judicial court and would depend on the relevant facts and circumstances of each case.

As section 64(3A) is a summary doxing offence, a suspect is liable for both civil and criminal penalties. If convicted of a summary offence under section 64(3A), a suspect is liable to receive a maximum fine of one hundred thousand (100,000) HKD for the civil penalty, and a maximum imprisonment sentence of two years for the criminal penalty.

Under section 64(3C), the second tier of indictable offence addressing doxing is as follows:

> A person commits an offence if—
>
> (a) the person discloses any personal data of a data subject without the relevant consent of the data subject—
>
> > (i) with an intent to cause any specified harm to the data subject or any family member of the data subject; or

(ii) being reckless as to whether any specified harm would be, or would likely be, caused to the data subject or any family member of the data subject; and

(b) the disclosure causes any specified harm to the data subject or any family member of the data subject.

In addition to consisting of the same thresholds and element as presented in section 64(3A), an indictable offence under section 64(3C) provides an additional fourth threshold which is actual harm having already occurred to the data subject or any of their family member. This specified harm needs to occur as a consequence of the suspect having intent to cause harm, or having acted in a reckless manner in carrying out the non-consensual disclosure of personal data of the data subject.

Similar to section 64(3A), section 64(3C) carries both a civil and criminal penalties. As section 64(3C) is an indictable offence, the penalties it carries are more severe than the penalties for a summary offence under section 64(3A). If convicted of an indictable offence under section 64(3C), a suspect is liable to receive a maximum fine of one million (1,000,000) HKD for the civil penalty, and a maximum imprisonment sentence of five years for the criminal penalty.

2.2.2. Powers to investigate and prosecute doxing cases

In addition to criminalising doxing, the 2021 Amendment conferred powers to the HKPPD that empower them to conduct criminal investigation on doxing cases, as well as to prosecute doxing cases. These powers are covered in four separate sections including section 66D, section 66G, and section 66H which cover the powers to conduct criminal investigation, as well as section 66C which covers the powers to prosecute doxing cases.

Under section 66D, section 66G, and section 66H, the HKPPD is conferred statutory powers to conduct criminal investigation into doxing cases. First, section 66D covers the HKPPD's powers to require a person to provide materials and assistance to facilitate a criminal investigation in relation to a potential doxing offence. Under section 66D(1), the HKPPD has the powers to require materials and assistance in relation to a specified investigation from relevant persons if the HKPPD reasonably suspects that a person may have possession of any material that is relevant to the investigation, or that a person may be able to assist in the investigation. The term "specified investigation" is clarified under section 66C as referring to an investigation relating to offences, which also include the two-tier doxing offences under section 64(3A) and section 64(3C). The HKPPD can directly gather any potential evidence or information from any relevant person which the HKPPC believes can help with the process of investigating a doxing offence under section 64(3A) and section 64(3C), without having to confer the investigation of the case to the HKP.

Under section 66D(2) in relation to conducting a criminal investigation, the HKPPD has the powers to require a person to provide relevant materials, attend before the HKPPD and answer questions, answer relevant written questions, make a statement in relation to the investigation, and give any relevant assistance as required. The term "material" used here refers to any document, information or thing. The HKPPD can exercise these powers through issuing a signed written notice with specified form, purpose, and details of the materials and assistance to be provided. The HKPPD can require a person to hand over any document, information, or item which the HKPPD has reason to believe would be relevant to the investigation process. There is no clarification or guidance provided on how the HKPPD sets the parameter for determining what material or assistance would be relevant to a potential criminal investigation.

Under section 66E, if a person fails to comply or provides false material in relation to assisting in a criminal investigation as required by the HKPPD, that person is liable for both summary and indictable offences. If convicted of a summary offence, the person is liable for a maximum fine of fifty thousand (50,000) HKD for civil penalty, and a maximum term of imprisonment of 6 months for criminal penalty. If convicted of an indictable offence, the person is liable for a maximum fine of two hundred thousand (200,000) HKD for civil penalty, and a maximum imprisonment term of 1 year for criminal penalty. These powers to require assistance or materials can be exercised with a written notice signed by the HKPPD themselves without a warrant from the judicial court.

Second, section 66G covers the HKPPD's powers to search premises and seize materials for the purpose of an investigation. Under section 66G, a warrant to access and investigate a premise may be granted if a court magistrate is satisfied with certain conditions. These conditions are that there is a reasonable ground to suspect that an offence, such as the doxing offences under section 64(3A) and section 64(3C), has occurred, is occurring, or will occurring in the future, and that there are potential materials in a premise or in an electronic device that are relevant to the case being investigated. In addition, the HKPPD, under warrant, may enter and search the premise, carry out investigation in the premise, as well as seize, remove, and detain any material in the premise for the purpose of conducting an investigation. Moreover, the HKPPD, under warrant, may access, seize, detain, decrypt, search, reproduce, copy, extract, and make into written form any material on an electronic device relevant an investigation.

There are certain cases where the HKPPD can access an electronic device without a prior issued warrant from the court. In relation to investigating an offence, such as the doxing offences under section 64(3A) and section 64(3C), the HKPPD may access an electronic device without a warrant if there is reason to believe that an

offence has occurred, is occurring, or will occur in the future, and that there is reason to suspect that any potential material is stored on the electronic device, and that a delay caused by the process of obtaining the warrant defeats the purpose of accessing the device. If the HKPPD reasonably believes that a delay would impede or hinder the investigation, they could legally access a person's electronic devices without first obtaining a warrant.

Third, section 66H covers the HKPPD's power to stop, search, and arrest persons for the purpose of an investigation. Under section 66H, the HKPPD may, without prior warrant, stop, search, and arrest any person whom they reasonably suspect to have committed offences such as the doxing offences under section 64(3A) and section 64(3C). In addition, the HKPPD may use reasonable force in the search or arrest in situations where the person resists or attempts to evade the efforts of search or arrest. In this process, the HKPPD may also take possession of any item found on the person or at the place of their search or arrest if there is reason to suspect that the item is related to the offence the person is being arrested for, or that the item would provide insights to the arrested person's character. Under these circumstances, the arrested person can be detained for up to 48 hours without charges.

If a person, without lawful excuses, obstructs, hinders, or resists the HKPPD in their exercise of powers under section 66G and section 66H, that person is liable for both civil and criminal penalties. Under section 66I, that person who is found guilty of an offence of non-compliance can receive a maximum fine of ten thousand (10,000) HKD for civil penalty, and a maximum imprisonment term of 6 months for criminal penalty.

Fourth, section 66C covers the HKPPD's power to prosecute doxing cases. The HKPPCD has the power to prosecute cases relating to offences or cases related to conspiracy to commit offences such as the doxing offence under section 64(3A).

However, the HKPPD can only prosecute cases related to summary offences. Cases relating to more serious offences such as the doxing offence under section 64(3C) cannot be prosecute directly by the HKPPD, and need to be conferred to the HKP for follow ups and further investigations.

2.2.3. Powers to issue cessation notices in doxing cases

The HKPPD is also given the powers to issue cessation notices under section 66M. If the HKPPD has a reasonable ground to believe that there is a written or electronic message with doxed information, and a Hong Kong person is able to take a cessation action in relation to that written or electronic message, then the HKPPD may serve a written notice to that person to take cessation action. Under section 66L, a cessation action refers to any action taken to cease or restrict disclosure of written messages. As for electronic messages, a cessation action refers to any action taken to remove message from an electronic platform, cease or restrict access to message on an electronic platform, or discontinue hosting the platform where the message is published.

A cessation notice has extra-territorial power and application. The HKPPD may also serve a written notice to a service provider to take cessation action only in relation to an electronic message with doxed information if the service provider is able to take a cessation action. This applies to non-Hong Kong service providers, regardless if they are situated in Hong Kong or not. A non-Hong Kong service provider refers to a non-Hong Kong person that has provided or is providing any service to a Hong Kong person. So as long as a person is able to take cessation actions, they can be served with a written cessation notice regardless if they are in Hong Kong or outside of Hong Kong. A person can appeal a cessation notice within 14 days of the written notice being served. However, the appeal does not affect the operation of the cessation notice in the meantime.

Under section 66O, if a person fails to comply with a cessation notice, they are liable for both civil and criminal penalties. They can also be liable for more serious penalties for each subsequent failure to comply with a cessation notice. For the civil penalty, the maximum fine for the first offence is fifty thousand (50,000) HKD, and an additional daily fine of one thousand (1,000) HKD for every subsequent day the offence continues. After the first offence, the maximum fine a person is liable to receive for each subsequent conviction of offence is one hundred thousand (100,000) HKD, and an additional daily fine of two thousand (2,000) HKD for every subsequent day that the offence continues. For the criminal penalty, the maximum imprisonment term for the first offence is 2 years, and the maximum of imprisonment term for each subsequent offence is also 2 years. If a person complies with a cessation notice, they will not incur any civil liability that arise out of contract, tort, equity, etc. towards another person due to their compliance with the cessation notice.

2.3. Doxing in Hong Kong after the 2021 Amendment came into effect

After the 2021 Amendment came into effect in October 2021, efforts by law enforcements in tackling doxing in Hong Kong saw a notable shift. Within a period of approximately 9 months before the 2021 Amendment came into effect on 8 October, the HKPPD received and handled 423 doxing cases. During this period, the HKPCPD also contacted online platforms 104 times with the requests to remove a total of 1,749 web links with doxed information or contents related to doxing, all of which were later removed from the online platforms. Within a period of approximately 6 months from October 2021 to March 2022 after the 2021 Amendment came into effect, the HKPPD received and handled 928 doxing cases. Within the same period, the HKPPD exercised the statutory powers conferred upon them through the issuance of 602 cessation notices to remove a total of 3,110 web links with doxed information.

In comparison to the number of cases in the period before the 2021 Amendment came into effect, not only did the number of doxing cases that the HKPPD handled more than doubled, but this also occurred over a shorter period of time. After the 2021 Amendment came into effect, the HKPPD has responded to more doxing cases within a period of 6 months when compared to the number of cases the HKPPD was able to respond to in the period of 9 months prior. When compared with the number of doxing cases during the period from mid-2019 to mid-2020, the number of doxing cases received and handled by the HKPCPD was still lower. However, the number of doxing cases reported after the 2021 Amendment came into effect was recorded in a six-month timeframe instead of the 12-month timeframe as recorded from mid-2019 to mid-2020.

With the statutory power conferred upon the HKPPD to restrain and take down doxed information through the issuance of cessation notices, the HKPPD was able to issue cessation notices and removed approximately twice the number of doxed information when compared to the 9 months period before the 2021 Amendment came into effect. The HKPPD was only able to remove a total of 1,749 web links with doxed information in the period of 9 months prior to the 2021 Amendment coming into effect. In comparison, the HKPCPD was able to remove a total of 3,110 web links in the period of 6 months that came after. The number of web links with doxed information that were taken down after the 2021 Amendment came into effect almost doubled the number of web links that were taken down in the period when doxing cases was at its height in Hong Kong. Within the period between mid-2019 and mid-2020, or approximately 12 months, the HKPPD was only able to remove 1,777 web links with doxed information out of 2,867 requests that were made to the online platforms. By comparison, after the 2021 Amendment came into effect, the HKPPD was able to remove a total of 3,110 web links with doxed information within a period of approximately 6 months. The removals of doxed

information in the period after the 2021 Amendment came into effect were all successful when compared to the 62% successful removals of doxed information in the period between mid-2019 and mid-2020.

The HKPPD has also exercised the newly conferred statutory powers to initiate 65 cases of criminal investigations related to doxing within the 6 months period after the 2021 Amendment came into effect. Prior, the HKPPD did not have the authority to directly conduct criminal investigations with regards to doxing cases. The HKPPD had only conducted preliminary investigations for cases which they suspected before referring any viable cases to the HKP to follow up on and further investigate. For instance, in the period of two years between mid-2019 and mid-2020, out of the 7,372 doxing cases which the HKPPD received and handled, 1,402 of these cases were referred to the HKP for further investigations. Similarly, out of the 957 doxing cases which the HKPPD received and handled in the period between mid-2020 to mid-2021, the HKPPD referred 59 of these cases to the HKP for further investigations.

Within the two years period before the 2021 Amendment came into effect, the HKPPD did not conduct any criminal investigation. After the conference of statutory powers in the 2021 Amendment, the HKPPD has initiated and conducted criminal investigations directly on their own without having to initiate the process and then refer cases to be investigated further by another entity. The HKPPD was able to initiate and conduct more investigations into doxing cases within a period of 6 months after the 2021 Amendment came into effect than within the period of 9 months prior to that.

After the 2021 Amendment came into effect, the HKPPD was also able to exercise the newly conferred statutory powers to conduct criminal investigations and prosecute persons suspected of having committed acts related to doxing. Just over a period of two months after 2021 Amendment came into effect, the HKPPD made

its first arrest of a person suspected of having committed a doxing offence contrary to the new section 64(3A) of the 2021 Amendment on 13 December 2021. Following this first arrest up until November of 2022, the HKPPD published media statements relating to 8 more subsequent arrests. All of these arrests were related to suspicion of violating section 64(3A) of the 2021 Amendment, which is non-consensual disclosure without actual harms having occurred, and is also a criminal offence under this section. Furthermore, on 6 October 2022, the HKPPD made a media statement announcing that the first conviction of a doxing case was made. The conviction was against a 27 years old male who pled guilty to seven charges under section 64(3A) relating to non-consensual disclosure of personal data. This case was adjourned and is pending a sentencing hearing at the end of the year. All cases which are mentioned above have not underwent a final sentencing hearing; thus, there are no publicly available court documents or judicial opinions which can be analysed as of yet.

Under the new section introduced by the 2021 Amendment, the HKPPD essentially has been conferred statutory power of conducting criminal investigation which is equivalent of the power of the HKP in conducting criminal investigation. This conference of statutory power is reflected in the HKPPD's ability to make arrests on the ground of reasonable suspicion of having committed a doxing offence. The HKPPD has the powers to make these arrests, in addition to being able to stop and search suspected individuals, without first obtaining issued warrants from the court.

In addition to the powers to conduct criminal investigations, the HKPPD has been conferred powers to prosecute summarily offences related to doxing acts, as seen with a conviction being secured under section 64(3A), which carries both a maximum civil fine of one thousand (1,000) HKD and a maximum imprisonment sentence of 2 years. However, the powers to prosecute are only applicable to summary offences, for instance, such as under section 64(3A) which is a summary

doxing offence with no actual harms having had occurred. The HKPPD can prosecute summary doxing cases without having to go through the process of conferring cases to the HKP for further investigation.

3. Conclusion

In summary, the research findings presented in this chapter are sectioned into three parts which aim to answer to the research questions raised for this research study. These three sections are presented in a chronological order. The first section presented relevant key findings during the period before the 2021 Amendment came into effect. First, doxing cases comprised of the majority of complaint cases received and handled by law enforcements from 2019 to 2021. Second, a majority of doxing cases in 2019 concerned the doxing of law enforcement officers. Third, a majority of Hong Kong people had experienced misused of personal data and were in support of amendments being made to the PDPO to address doxing in 2020. The second section presented relevant key findings on the legal changes that were introduced to address doxing in Hong Kong. It presented three changes that was introduced in the 2021 Amendment to response to the increased number of doxing cases. First, a two-tier offence system was introduced to criminalise doxing. Second, the HKPCPD was conferred powers to conduct criminal investigations and prosecute doxing cases. Third, the HKPCPD was conferred powers to issue cessation notices to remove doxed information. The third section presented relevant key findings on the law enforcement's response to doxing after the 2021 Amendment came into effect. First, the number of doxing cases received and handled by the HKPCPD was at its highest within a six-month timeframe after the 2021 Amendment came into effect. Second, the HKPCPD began to directly conduct criminal investigation and prosecute doxing cases without needing to confer cases to the HKP after the 2021 Amendment came into effect. Third, the HKPCPD had

been successful in removing contents related to doxing through issuing cessation notices to online service providers after the 2021 Amendment came into effect.

Chapter 5: Discussion

1. Introduction

This chapter discusses the key findings of this research study that is presented in the previous chapter. There are three research questions that this research study raised with the aims of 1) investigating and examining doxing and the effects it has in the context of Hong Kong, and 2) investigating and understanding how doxing is legally addressed in the context of Hong Kong. The three research questions are: 1) What are the challenges that doxing posed to law enforcement?; 2) How has doxing in Hong Kong been addressed by the 2021 Amendment?; and 3) What are law enforcement's response to doxing after legal changes were made to address doxing?

This research study identifies seven findings which answer to the three research questions. The first finding is that doxing cases comprised of the majority of complaint cases received and handled by law enforcements from 2019 to 2021. The second finding is that a majority of doxing cases in 2019 concerned the doxing of law enforcement officers. The third finding is that a majority of Hong Kong people had experienced misused of personal data and were in support of amendments being made to the PDPO to address doxing in 2020. The fourth finding is that Hong Kong has introduced the 2021 Amendment as a response to combat doxing in Hong Kong. The fifth finding is that the number of doxing cases received and handled by the HKPCPD was at its highest within a six-month timeframe after the 2021 Amendment came into effect. The sixth finding is that the HKPCPD began to directly conduct criminal investigation and prosecute doxing cases without needing to confer cases to the HKP after the 2021 Amendment came into effect. The seventh finding is that the HKPCPD had been successful in removing contents related to doxing through issuing cessation notices to online service providers after the 2021 Amendment came into effect.

The discussion in this chapter is divided into three sections, with each discussing a research question and its relevant findings. The first section discusses the first research question as well as the first, second and third key findings. The second section discusses the second research question as well as the fourth research finding. The third section discusses the third research question as well as the fifth, sixth and seventh research findings. Finally, the key discussion points will be briefly summarised in the conclusion section.

2. Discussion of the research questions and key findings

2.1. The challenges posed by doxing to law enforcement

There are three key findings which are relevant in answering to the first research question. The first finding is that doxing cases comprised of the majority of complaint cases received and handled by law enforcement between 2019 and 2021. In 2019 alone, the number of doxing cases received by the HKPCPD was at an all-time high. As there were no data published on how many doxing cases the HKPCPD had received in the previous years, the sudden spike of the number of doxing cases in 2019 suggests that doxing had not become prevalent before then. This sudden increase in the number of doxing cases can be attributed to the 2019 protest movement during this period of time. Between 2019 and 2021, more than a quarter of all types of complaints were attributed to doxing cases. This sudden emergence and continuation of this practice posed a challenge to Hong Kong law enforcement which suddenly had to handled and responded to an unprecedented number of doxing cases, an issue that was never highlighted before then. However, it is not to suggest that doxing had not existed in Hong Kong prior to this time period. The practice of searching for and disclosing personal data had been a part of Hong Kong society before 2019. It had only been confined to smaller communities, such as in a school environment, where students were beginning to

use more social media platforms and participated in a culture of searching and disclosing personal data of their peers in through deanonymizing doxing.

Prior to the case of Hong Kong in 2019, there had been no previous cases documented in the literature on the doxing target whereby the number of doxing cases suddenly and rapidly increase in number within a short period of time. However, given the nature of doxing, a possible and reasonable explanation could be drawn from existing literature. One of the motives that can prompt an individual to dox others is vengeance or justice seeking. The 2019 protest movements had created an atmosphere of social unrest, as well as mounting tensions not only between protesters and law enforcements, but those who respectively supported and sympathised with each side as well. With each side having held their own firm beliefs to their cause and their duty, it is quite easy to see the how doxing could have been motivated and perpetuated during this period of time. However, it would be more accurate to attribute a majority of these doxing cases to targeted doxing due to the context and nature of the majority of cases.

The second finding that answers to the first research question is that a majority of doxing cases in 2019 revolved around law enforcement officers. Out of all the doxing cases received and handled during this timeframe, approximately 80% of these cases were related to law enforcement officers and their family members. Doxing had emerged as a strategic tactic in response to the various instances of use of force by police officers against unarmed protesters. These police officers, as well as their family members, were subjected to efforts of targeting doxing. This had not only exposed personal data that could be used to identify and locate these individuals in the real world, but this disclosure had also increased their visibility to a contentious online mob that were seeking some form of retribution for what they would view as an unjustified use of force. Not only were law enforcement having to handle and response to doxing cases reported by the Hong Kong public,

but these law enforcement officers had to also deal with the consequences of them and their family members becoming the doxing targets as well.

The family members of these law enforcement officers could be considered as innocent parties that were implicated in these doxing cases. They had suffered indirect harms, had themselves become the doxing targets through their known affiliations or relations with the policer officers who were at the primary doxing targets. Innocent parties being implicate in doxing cases can be due to a few reasons. First, they can be implicated in doxing cases in an indirect manner. An innocent party can become the doxing targets not because they have committed any actions or said anything that elicited a doxing response. Instead, they can potentially be doxed due to their association with someone or something else that instigated a doxing response. In other words, they could be doxed for simply being affiliated with someone or something else that is the true source of the ire of the doxer. Second, innocent parties can be implicated in doxing cases due to misinformation. Doxers can unintentionally dox the wrong target, either due to mistaken identities or being misinformed of the context that instigated a doxing response in the first place. In other words, an innocent party can be doxed because they had been mistaken by the doxer for someone else, or that the doxer had misinterpreted the situation that led them to doxed someone.

These scenarios of innocent parties being implicated in doxing cases are likely to occur due to the nature of the medium of doxing - the cyberspace. First, the culture of information sharing in the cyberspace can allow an individual's activities, affiliations and opinions to be observed by other users in the cyberspace. It is not out of the norm to see someone on a social media platform sharing their daily activities, work achievements, or expressing their opinions on a subject matter. It is not difficult to observe or infer an individuals' affiliations as well as their views on a subject matter through these public posts. It is through these observations and

inferences that an innocent party who did not commit any wrongdoing can suddenly find themselves at the receiving end of a doxing effort. A doxer might not have any intent to specifically dox the innocent party, but through targeting that individual's affiliations, there is a chance that the innocent party will be harmed.

Second, the culture of rapid and viral information sharing in the cyberspace also holds the potential for misinformation to be spread. It is not uncommon for two or more people to have the same legal names, or to have other similar identifying features such as physical appearances. The same could occur in the cyberspace where people from all over the world can exist and interact with one another through their online identities. In this interconnected space, it is reasonable and not out of the realm of expectation to find online accounts with the same user names that may correspond to their real legal names, or to find profile pictures of users with similar identifying features. Given that the cyberspace also offers a veil of anonymity and allows an individual to have multiple unrelated accounts, these users can also embody different personas or impersonate another individual entirely. It is easy for an individual's online posts or activities to be taken out of context in the cyberspace. Given the nature and culture of information sharing on online platforms and forums, an individual's posts or activities can be shared multiple times by other online users. The information can be shared to all different types of groups and communities repeatedly over and over again. This can lead to a situation of context collapse where information is interpreted out of context or based upon false assumptions or beliefs. This environment of anonymity and misinformation can easily lead a doxer to operate upon false or misleading information, and end up targeting an innocent party in the process.

The third finding that answers to the first research question is that a majority of Hong Kong people in 2020 had experienced misused of personal data and were in support of amendments being made to the PDPO to address doxing. Even after the

social unrest that was caused by the 2019 protest movements had died down, the Hong Kong people were still experiencing misuses of personal data whereby more than a third of the people surveyed had reported negative experiences with regards to misuses of their personal data. This suggests that even in the absence of an event that had elicited mass doxing responses, doxing had become a part of the Hong Kong society whereby the general populace was still having negative experiences with their personal data being misused a year later. Personal data is a crucial element that is widely known to have been weaponised by doxers, especially during the period of social unrest in Hong Kong. The resulting harms can vary from mild inconveniences to the data owner to extreme instances of real-world harassments. However, the harms from misuses of personal data may just be an inadvertent consequence. In other words, harms may not have been intended or may have been an unforeseen result of the misuses of personal data.

Among the Hong Kong people who had reported misuses of their personal data, only 11% of them had made official complaints to the HKPCPD. Those who did not lodged officially complaints provided three reasons. First, they did not know where to lodge the complaints. Second, they perceived the process of lodging a complaint as too troublesome. Third, they perceived the issue as unimportant to be spending time on. This suggests two implications. The first implication is that there is an overwhelming number of cases which had happened unnoticed and unaddressed by law enforcement. This further implies that the number of cases officially documented and presented by the HKPCPD did not truly reflect the reality of what was occurring in Hong Kong, at least during the 2020 timeframe. This might be the reason for the sharp drop from 2019 in the number of doxing cases. The second implication is that there were barriers or difficulties in accessing recourses that can help address the problem. The three reasons provided vary slightly from the reasons reported in the literature on doxing. In the case of Hong

Kong, a majority of those who did not lodge an official complaint were still seeking ways to legally address their situation. In the literature, cases of doxing generally go unreported due to victims not knowing there can be recourses to help them with their situations, or that the victims are deterred from reporting their situations due to fear or shame. In some instances, victims simply perceived that their experiences and situations do not warrant law enforcement intervention. This reflects the reason given by some Hong Kong respondents in the survey who experience of misuse of information, but did not think it was an issue that needed to be addressed. This further suggests that there is a wide range of the severity of harms that victims of doxing can experience, and that the victim experiences are not confined to any certain threshold.

These negative experiences combine with the high number of doxing cases that occurred during 2019 suggest that this practice had become an issue of concern for not only for the Hong Kong populace who were experiencing them, but for law enforcement as well as they were unable to address these unreported cases. This may have been a reason that had led some people in Hong Kong to support changes to be made to legally addressing doxing. Almost half of the Hong Kong peoples who were surveyed strongly support the introductions of legal measures to address doxing. During this timeframe, there were no legal measures to address doxing in Hong Kong yet. This lack of legal measures and the concerns among the public serve as a basis and rationale to introduce changes to answer to the need in addressing this issue. This aspect is also reflected in the literature on doxing as there been growing concerns among scholars concerning the lack of legal remedies and measures to address doxing. This suggests that doxing in Hong Kong during this timeframe aligns with the general practice of doxing in contemporary literature, especially with regards to the lack of legal remedies and measures against doxing.

2.2. Legislative amendment to address doxing

In answering to the second research question, this research study found three relevant changes that were introduced in the 2021 Amendment to address doxing. The first change is that doxing is criminalised as a punishable offence. Hong Kong law makers had chosen an interesting approach to address doxing by criminalising it as an offence under a privacy and data protection law. Although the weaponization of personal data and issues posed to an individual's privacy and anonymity have been discussed in the literature on doxing, there have not been any discussion or observation on legally addressing doxing under a privacy or data protection law. Personal data has been a crucial element in the discourse of harms and how harms are caused through doxing. This provides a rationale and basis for Hong Kong law makers to make doxing an offence under a privacy and personal data law. Given the consequences and harms of doxing are not confined just within the cyberspace, the choice to address doxing under a privacy and data protection law could arguably provide a wider scope of applicability as to the coverage of doxing offences. For instance, if an individual experiences harassment and attack in the real world after having been doxed, this incident goes beyond the scope of cyber harassment where the harms done are confined to the realm of the cyberspace.

The element of intent is also another crucial threshold in the doxing offence under the 2021 Amendment. Although it is generally a common element and legal test to prove an individual's guilt in committing an offence, the intent to commit doxing is not as frequently discussed in the literature. The motive to commit doxing is a more frequently discussed element that also distinguishes doxing from other similar cyber offences. There is a distinction to be made between intent and motive. Under criminal law, intent refers to an individual's state of mind during the time an offence is committed, whereas motive refers to the reason that made an individual commit an offence. Thus, the element that is addressed under the 2021 Amendment is an individual's mental state of whether or not they were in a reckless state of mind

when disclosing another individual's personal data. The motives of the doxer may be relevant to establishing their intent, but it is not always the case since the intent needs to be reckless in nature in order for the disclosure to qualify as a doxing offence.

Another aspect in criminalising doxing as an offence under the 2021 Amendment is the introduction of a two-tier system that is punishable by both civil and criminal penalties. The two tiers of doxing offence are differentiated by the presence of actual harm. The doxing offence is more severe and becomes an indictable offence when actual harm has occurred as a consequence of the doxing. Given that literature on doxing identifies a wide range of motives and harms with regards to doxing, having this two-tier system to differentiate the types of offence allows the scope of the offence to cover all severity of doxing case, and not disregard the less severe ones. A summary offence for less serious cases still allows victims to seek justice in a manner that does not take up too much time or resource from more serious cases of indicatable offences where the victims have suffered actual harms. Thus, narrowing the scope of applicability of the doxing offence may exclude or disregard a portion of what could still be considered as doxing within the general literature.

The second change that is introduced in the 2021 Amendment is the conference of power to the HKPCPD to investigate and prosecute doxing cases. With their roles being in relation to the enforcement and implementation of the PDPO, the HKPCPD is within the scope to be conferred power to conduct criminal investigation and prosecute doxing cases. As previously discussed, 42% of Hong Kong people who were surveyed in 2020 was fully in support of allowing the HKPCPD to wield this authority to directly conduct criminal investigation and prosecute doxing cases. This suggests that some of the Hong Kong people believe that the conference of these powers to the HKPCPD is necessary and reasonable to combat doxing in Hong Kong.

Within their powers to conduct criminal investigation, the HKPCPD has the authority to require any person to provide assistance and materials to facilitate the process of investigating doxing cases. Any failure to comply with the HKPCPD's requirement for assistance and material or impede the investigation process would constitute as a non-compliance offence. The offence of knowingly interfering or obstructing the process of lawful investigation typically carries both civil and criminal penalties, especially in the process of criminal investigation. This is to ensure that law enforcement can effectively and efficiently respond to criminal cases which is more serious and severe in nature. Having this incentive in place would encourage people to comply and assist with the investigation process, or at least to not hinder or waste law enforcement's effort.

The scope of the HKPCPD's powers to conduct criminal investigation also includes the authority to access and investigate a premise with an issued warrant. The HKPCPD can seize and access any electronic device found in the process which they suspect to have relation to the case being investigated. To obtain such warrant, the HKPCPD needs to provide the issuing judge with a reasonable ground of suspicion as to why a warrant is necessary to access a premise to conduct investigation or gather potentially relevant evidence in related to a criminal investigation into doxing cases. This suggests that by simply suspecting that a doxing offence has occurred, is occurring, or will occur, and that there are potential evidences in a premise, the HKPCPD can gain access and seize materials in that premise. Although this creates a picture of intrusive use of the HKPCPD's authority, it should be noted that this can only be done under a warrant. The HKPCPD has to make a reasonable case to utilise these powers to access and investigate an individual's premise to a judge to obtain this warrant. The presiding judge has to then evaluate and make a decision as to whether it is necessary and

appropriate to grant a warrant of this nature. However, there is ground for the HKPCPD to access an electronic device without a warrant.

The HKPCPD can access an electronic device without a warrant if they reasonably believe that there is any potential evidence relevant to investigating a doxing case and that the delay from the process of applying and waiting for a warrant would hamper or defeat the purpose of accessing the electronic device. On one hand, this is a reasonable basis and justification for accessing an electronic device without an issued warrant. Electronic data can easily and quickly be deleted from a device, and in some cases, the deleted data cannot be recovered by any means. It is not unreasonable to assume that a suspect may be aware or alerted to the criminal investigation and promptly take actions to cover their traces or remove any relevant evidence. To mitigate or prevent these scenarios from occurring and jeopardizing the investigation entirely, the HKPCPD needs to be able to react and response promptly to ensure that no evidence is lost or compromised.

On the other hand, the powers to access an electronic device without a warrant based solely on reasonable suspicion may present a picture of disproportionate use of power and infringement of an individual persona privacy. The notion of reasonable suspicion is subjective to one's judgement. What is reasonable to a law enforcement officer may not present with the same reasonability and rationality to an individual who has their personal electronic device seized and accessed without a warrant. Even the perspectives among law enforcement officers can shift and vary on the notion of reasonability. The 2021 Amendment does not provide any clarification or definition as to what determines and qualifies as reasonable suspicion. This further suggests that there is an issue of lack of standard or threshold to guide the law enforcement officers in determining what situation or circumstance would be necessary and appropriate in exercising these powers without needing an issued warrant. Although cases where these powers are exercised without an issued

warrant are the exceptions, they nevertheless raise concerns regarding the lack of a uniform standard to guide and inform the judgement of law enforcement officers in making decision preceding an issued warrant.

With their powers to conduct criminal investigation, the HKPCPD also has the authority to stop, search and arrest any individual without an issued warrant in relation to any suspect doxing cases. Similar to the authority to access an electronic device without an issued warrant, the HKPCPD can exercise the powers to stop, search and arrest if they reasonably suspect that an individual has committed, is committing, or will commit a doxing offence. In the process, the HKPCPD can seize and detain any item found on the individual at the time if they reasonably suspect that the item is relevant to investigating a doxing offence. The HKPCPD can also use force in cases where a suspected individual attempts to evade or resist complying with the exercise of these powers. This raises a few areas of concerns. Without an opportunity for a judge to evaluate the cases and issue a warrant, especially concerning the arrest of a suspected individual, it is questionable as to whether the exercise of these power is really necessary and appropriate. As previously discussed, the notion of reasonable suspicion is relatively subjective even among law enforcement officers. Without any guiding standard or threshold to determine if there is reasonable suspicion, there would be no uniformity in standard with regards to when this exercise of powers to stop, search and arrest is necessary and appropriate.

These doxing cases do not have to already happened for the HKPCPD to make an arrest. In other words, an arrest can still be made even if the HKPCPD only suspects that a person is about to commit a doxing act. This is a relatively broad scope of the HKPCPD's powers, as anyone can essentially be stop, search and arrest without a warrant based solely on the discretion of the arresting officers. On one hand, the HKPCPD being able to react and response promptly in this manner would be

beneficial to the investigation process without needing to risk the potential suspect destroying any evidence or fleeing to other territories where it may create difficulties in pursuing the case further. On the other hand, this scope of powers raises question regarding the proportionality, especially given that any non-compliance or hinderance would result in a non-compliance offence. A suspected individual, no matter their guilt or innocence, would be incentivised to comply with the arrest. If the suspected individual is innocent, this could potentially lead to inefficient utilization of resources as the law enforcement would be focused on a case where an innocent party is implicated instead.

The HKPCPD is also conferred the power to directly prosecute doxing cases. The scope of the HKPCPD's powers in this regard is only limited to summary offence related to doxing which does not require that any actual harms being involved. Thus, the HKPCPD can only directly prosecute the first-tier of doxing offence. This suggests a more efficient mechanism of handling the different tiers of doxing cases. This also allows less serious cases to be investigated and directly prosecuted by the HKPCPD without having the need to confer the cases further to the HKP. This suggests some benefits as this allows the HKPCPD to filter the less serious cases to be addressed more promptly and leaving more serious cases where victims would likely be looking for recourses and justice to the HKP.

The third change introduced in the 2021 Amendment is the conference of power to the HKPCPD to issue cessation notices in doxing cases. If the HKPCPD has reasons to believe that a written or electronic message contains doxed information and that a Hong Kong or non-Hong Kong person can take actions to remove the message, then the HKPCPD can issue a cessation notice to remove the message or restrict the dissemination of the message. There are a few implications in choosing to restrict the flow of information as a measure to combat the spread of doxing and the dissemination of doxed information. On one hand, it can help to mitigate the

harms of doxing by curbing the doxing effort at its initial stage. The harms that a doxing target experiences typically result from the mass dissemination of disclosed information on that individual. This not only causes psychological distresses towards to a doxing target, but this also heightens the doxing target's visibility and expose them to an unknown audience in the cyberspace. This exposure carries the risks of attracting the attention of bad actors who may seek to harm the doxing target through weaponizing the doxed information. By removing the doxed information or restricting further dissemination, the HKPCPD removes the potential doxers' ability to cause harms to the doxing target.

On the other hand, the HKPCPD's powers to require the removal of doxed information raises some concerns with regards to the freedom speech and expression. The removal and restriction of contents alone is tethering the line between mitigating measure to combat doxing and censorship. In the literature on doxing, discussions have been raised as to when a restriction of content and expression of others is appropriate and necessary as to not constitute an act of censorship. An argument has been made that although removing doxed information may to some extend impede upon an individual's freedom of speech and expression, it is a necessary compromise to be made to prevent further and more damaging harms to another.

Another aspect of the HKPCPD's powers to issue cessation notice is the scope and applicability of the cessation notice. A cessation notice has extra-territorial power and application. If an individual or service provider can take cessation action, the HKPCPD has the powers to issue a cessation notice to them to require the removal of doxed information. This is also applicable regardless of whether the individual or service provider are situated in Hong Kong territory or not. If the subject of the issued cessation notice fails to comply with the requirements laid out in the notice, they are liable for both civil and criminal penalties. If the subject fails to comply

more than once, they are can incur additional fines on a daily basis. This is a relatively strong incentive for the subject of the cessation notice to comply and remove the doxed information.

Although an appeal can be made within 14 days of being served, the cessation notice is nevertheless still in effect during that 14 days period. This implies that although an individual or service provider has the right to appeal against a cessation notice, they would still be subjected to the daily recurring fines beyond their first offence. There is no clarification as to whether the recurring fines would be waived in the event of a successful appeal. This suggests that there is a heavier incentive for the subject of the cessation notice to simply comply rather than risk being subjected to a recurring fine during the process of appealing. However, an argument can be made for instating immediate effect of the cessation notice which is to incentivise the subject of the cessation notice to promptly take actions to remove or restrict the dissemination of the doxed information. This prompt measure to restrict access and visibility of the doxed information would mitigate and prevent further harms that can be caused to the doxing target.

2.3.c. Law enforcement's response after the 2021 Amendment

There are three findings which are relevant in answering to the third research question. The first finding is that the number of doxing cases received and handled by the HKPCPD was at its highest within a six-month timeframe after the 2021 Amendment came into effect. During a period of six months after legal measures were introduced, the HKPCPD received and handled 928 doxing cases. Although this number is still relatively low compared to the cases between mid-2019 and mid-2020, it is still higher than the number of cases in the period of nine months prior. This suggests two implications. On one hand, this may suggest that the 2021 Amendment has made the Hong Kong people more aware of the available recourses to address any doxing experience they may have had. Not only can they seek justice

or other recourses for any harm they have experienced in relation to doxing, they can also take preemptive measures before the doxing can cause any actual harm to them. This may provide an incentive for the Hong Kong people to actively choose to report their experiences to the HKPCPD; hence, the increased number of cases in this shorter timeframe.

On the other hand, this increased in the number of cases may reflect more reporting of minor doxing cases or cases where investigations are initiated by the HKPCPD. As a summary doxing offence only requires intent and not actual harm to have been done, more cases in this nature may have been reported more in the wake of the 2021 Amendment. Moreover, as the HKPCPD is empowered by the 2021 Amendment to address doxing cases, it is reasonable to assume that the HKPCPD has taken more initiatives in investigating potential doxing cases that might constitute a doxing offence. Without the need to confer less serious cases to the HKP, it is likely that the HKPCPD may have been able to more address more cases in a shorter timeframe as well. This implies an efficient utilization of resources such as time and human resources, and allow more capacities for the HKPCPD to address more cases.

The second finding is that the HKPCPD has begun to directly conduct criminal investigation and prosecute doxing cases without needing to refer cases to the HKP. Within a span of a year, the HKPCPD has made conducted nine arrests for criminal investigations relating to doxing cases, and successfully made one conviction for a doxing offence. This suggests that the 2021 Amendment was effective in some capacity in empowering the HKPCPD to crack down on doxing cases. This further suggests that the HKPCPD has taken firm initiatives in addressing doxing cases in their exercise of the conferred powers. Bringing the first conviction in a doxing case would suggest to the public that the issues posed by doxing are being taken

seriously, and also serves as a warning to any potential offender that there are now serious ramifications for committing a doxing offence.

Although the HKPCPD demonstrates that doxing is now being taken more seriously through making several arrests and a conviction, this also raises concerns as to the actual scope and effectiveness of these conferred powers. Thus far, it is possible to discern that all the arrests and the single conviction were made on suspicions of having intent to commit doxing acts with no harms having had occurred. However, for the cases in which the suspects were charged as well as the one case where a conviction was made, there were no further explanations or elaborations on the details of the charges. Without further information or clarification on the specific details of each cases, it is not possible to ascertain the actual scope and effectiveness of the HKPCPD's conferred powers in addressing doxing in terms of investigating and prosecuting doxing cases.

The third finding is that the HKPCPD had been successful in removing doxed information through issuing cessation notices. The HKPCPD has removed twice as many doxed information's in the six months after the 2021 Amendment came into effect when compared to the nine months prior. In contrast, the HKPCPD was only moderately successful in requesting online platforms to remove doxed information prior to the introduction of the 2021 Amendment. The high number of doxed information that the HKPPD was able to remove within a short timeframe suggests that the HKPCPD's exercise of the powers to issue cessation notice is effective in some capacity in requiring compliance to restrict the spread of the doxed information.

The removals of doxed information in the period after the 2021 Amendment were all successful when compared to the 62% successful removal of doxed information in the period between mid-2019 and mid-2020. This suggests that online platforms with web links related to doxed information showed less, if not no reluctance, in

complying with the HKPPD in removing doxed information from their platforms. The reason for this may have been due to the penalties of non-compliance with the cessation notice, especially the potential to incur daily fines even in cases where the subject of the cessation notice wants to appeal. As discussed previously, this provides the subject of the cessation notice, especially the service providers, with a stronger incentive to promptly comply instead of going through the appeal process.

3. Conclusion

To summarise, this chapter has discussed the key findings which are relevant in answering to the aims and objectives of this research study. The discussion is divided into three sections, with each section answering to one of the three research question. The first section discussed the challenges that doxing posed to Hong Kong law enforcement, specifically the HKPCPD. The key findings suggested that doxing has become a prevalent issue in Hong Kong after the 2019 protest movement. During the time when doxing was at its peak in 2019, law enforcement officers were the primary targets of targeting doxing. Their family members who were innocent parties also became targets of doxing through their affiliations with targeted officers. Moreover, even after the atmosphere of social unrest has subsided, doxing remained a commonly observed practice in Hong Kong. The second section discussed the legislative amendment to address doxing in Hong Kong. There are three changes that were introduced in the 2021 Amendment. There are elements that were introduced in the 2021 Amendment reflected upon and aligned with elements that have been previously discussed within the literature on doxing. However, there were also elements that have not been thoroughly discussed in relation to the issues posed by doxing. The third section discussed the effects of the 2021 Amendment in addressing doxing. The key findings suggests that the changes introduced were effective in some capacity in addressing doxing. The increased in number of cases suggested that either doxing cases were reported more

frequently or that the HKPCPD has initiated more investigations into doxing cases. Although the HKPCPD has been empowered to combat doxing, the actual applicability and scope of their powers raised concerns, some of which are reflected in the literature on doxing.

Chapter 6: Conclusion

1. Introduction

This chapter provides a summary of the findings of this research study in relation to the research aims and research questions. It also outlines the values of the findings of this research study and the contributions to the existing literature. This chapter also provides a review of the limitations in conducting this research study, as well as proposing recommendations for future studies.

The summary of this research study is divided into three sections. The first section discusses the key findings of this research study and how they serve to answer to the aims and questions of this research study. The second section reviews the limitations of this research study. The third section discusses recommendations based on the findings of this research study for potential future studies. Lastly, this chapter concludes by briefly summarise the discussion points in this chapter.

2. Summary of research findings in relation to the research aims and questions

The relevant findings of this research study are divided into three sections that answer to the aims of 1) investigating and examining doxing and the effects it has in the context of Hong Kong, and 2) investigating and understanding how doxing is legally addressed in the context of Hong Kong. Each section aims to answer to one of the three research questions of this research study. The first section aims to answer the question of what are the challenges that doxing posed to law enforcement? It presents an analysis of doxing in Hong Kong prior to the 2021 amendment, including an examination of the PDPO as the base legislation for amendment, as well as doxing in Hong Kong before the 2021 Amendment. There were three relevant key findings which answer to this question. First, the number of doxing cases was at an all-time high during the period before the 2021 Amendment came into effect. It is found that before the 2021 Amendment came

into effect, the high number of doxing cases has made doxing a prevalent issue in Hong Kong during this timeframe.

Second, the primary doxing targets during this period of time were law enforcement officers and their family members. A majority of these doxing cases falls under the category of targeting doxing, whereby the doxer specifically discloses the specific details of an individual's personal data which can be used to identify and locate the doxing target in the real world. This category of doxing is most prevalent during the period of the 2019 protest movement, and the majority of the doxing targets was law enforcement officers and their family members. The family members of the targeted law enforcement officers are innocent parties which were doxed through affiliations.

Third, doxing has become a prevalent issue even after the 2019 protest movement had died down. There was still a relatively high number of doxing cases being reported to the HKPCPD after the social unrest that triggered the rapid increase in doxing cases has subsided. This suggests doxing has become a prevalent issue within Hong Kong. Moreover, this also led to concerns and negative experiences of personal data misuse by the Hong Kong public. A majority of Hong Kong people who had experienced misuses of personal data did not file a complaint due to difficulties in accessing recourses to address their grievances or that they viewed the issue as not important enough to seek redress. Due to the prevalence of doxing cases and the negative experiences of personal data misuse, a majority of the Hong Kong people was also in support of introducing legal changes to the PDPO to address the increasing number of doxing cases.

The second section aims to answer to the question of How has doxing in Hong Kong been addressed by the 2021 Amendment? It presents an analysis of the 2021 Amendment through covering the three main changes that were introduced as a response to the increasing number of doxing cases in Hong Kong. First, the 2021

Amendment criminalised the doxing offences through introducing a two-tier offence system which includes a summary offence and an indicatable offence. The two-tier offence system serves to differentiate the different levels of offence by the severity of harms. A summary doxing offence only incorporates the element of intent to cause harm and does not include the threshold of actual harm having been caused by the doxing offence, whereas an indictable offence is more serious and includes both the thresholds of intent to cause harm and actual harm having been caused by the doxing offence.

Second, the HKPPD is conferred powers to conduct criminal investigation and prosecute doxing cases. The powers include search and arrest, access a premise with warrant, require a person to cooperate and assist, and seize materials related to the investigation, as well as prosecuting summary offences related to doxing. There are exceptional cases where the HKPCPD can exercise certain powers without first obtaining an issued warrant from court. These exceptions include the authority accessing an electronic device without a warrant if the HKPCPD has ground to believe that any delay would jeopardise the investigation, as well as the authority to stop, search and arrest an individual on the ground of reasonable suspicion that the individual has committed, is committing, or will commit a doxing offence. This authority to act based upon the discretion of the HKPCPD raises the questions of whether the actual scope powers within these exceptional cases is necessary and appropriate to allow the HKPCPD to more effectively combat doxing, or whether this can pose problems concerning censorship.

Third, the HKPPD is conferred powers to issue cessation notice. This allows the HKPPD to require a person or service provider, regardless if they are in or outside of Hong Kong, to restrict or remove doxed information related to a Hong Kong person. Failure to comply with a cessation notice from the HKPCPD is an offence in and of itself, which can incur heavier penalties after the first offence, including

a daily recurring fine. An appeal can be made against a cessation notice from the HKPCPD with 14 days, but the appeal process does not halt the applicability of the daily recuring fine. The nature of the appeal suggests that the recurring fines plays an element in incentivizing prompt compliance and disincentivizing against going through an appeal process.

The third section aims to answer to the question of what are law enforcement's response to doxing after legal changes were made to address doxing? It presents an analysis of doxing in Hong Kong after the 2021 Amendment came into effect, specifically looking at the difference in how the HKPCPD response to doxing. First, the number of doxing cases received and handled by the HKPCPD was at its highest within a six-month timeframe after the 2021 Amendment came into effect. It is found that although the number of doxing cases that the HKPPD received and handled were higher, especially in the period between mid-2019 and mid-2020, the HKPPD was able to more effectively and efficiently handled and responded to more doxing cases within a shorter timeframe after the 2021 Amendment was introduced. On one hand, it implies that introducing legal changes through the 2021 Amendment has made the Hong Kong people more aware of the available recourses and who to report to. On the other hand, it also implies that the increased in doxing cases can be attributed to the HKPCPD being empowered by to take more initiatives in investigating doxing cases.

Second, the HKPPD is able to conduct criminal investigations and prosecute summary offences directly without having to confer cases to the HKP. With the powers conferred by the 2021 Amendment, the HKPPD was able to initiate their own investigations into potential doxing cases and made arrests as well as a conviction for doxing offences. Although this demonstrates that doxing is being taken more seriously by the HKPCPD, the scope and application of these new powers are relatively unclearly due to the discretionary nature of the HKPCPD's

ability to exercise these powers. In terms of the powers to prosecute doxing offence, the HKPCPD is able to prosecute only summary doxing offence. This suggests some benefits as the HKPCPD can promptly address as well as filter out minor and less serious doxing cases and only confer serious cases to the HKP, which can result in better and more efficient use of law enforcement resource.

Third, the HKPCPD had been successful in removing contents related to doxing through issuing cessation notices to online service providers after the 2021 Amendment came into effect. Since the 2021 Amendment came into effect, the HKPPD is empowered to issue cessation notices and has removed more doxed information than in the years before, whereas requests to online platforms to remove doxed information were only moderately successful before the 2021 Amendment came into effect. Some of the online platforms were reluctant to comply before the 2021 Amendment came into effect, most likely due to reasons of user's data privacy as well as the concerns over freedom of speech and expression. After the 2021 Amendment came into effect, the online platforms fully comply with any of the HKPCPD's cessation notice as there is also a non-compliance offence regarding the cessation notice. The reasons for this might be that there are more incentives for the online platform providers to comply with the cessation notice, regardless if they have ground for appeal or not.

3. Limitations

There are certain limitations to the choices of this research study which need to be acknowledged. First, as this research study employs an inductive reasoning approach which can provide benefits through a bottom-up approach by making observations before generalizing an interpretation. However, this also presents an inherent weakness as although data or material observations maybe accurate, it does not mean that the interpretations or generalizations of the observations are universal. Moreover, the inductive reasoning approach is also limited as the

investigation is halted after an interpretation or generalised conclusion is reached, disregarding the possibility that this achieved result can still be proven otherwise if the investigation was to be continued.

This research study was also conducted based on qualitative research design which allowed the analysis and interpretation of qualitative data to potentially be highly subjective based on the researcher's individual philosophical worldview as well as being prone to inherent biases. Thus, in selecting the subject for this research study and determining the aims and objectives within it, the researcher attempted to select a subject matter of which she has had little to no prior familiarity with to mitigate any pre-existing bias from influencing the discovery and investigation of the phenomenon. Moreover, the selection of the subject for the case study was also intentionally done, as the examination and observation of legal documents provided limited room for interpretation unless cross referenced with other literature for discussion.

There are also limitations faced with regards to the process of data or material collection for the case study. With this research study having been conducted as desk-based research, the retrieval of data and materials used within the case studies were limited to what was made available on the public government data. Moreover, not all documents were made available to the public, and some were not available with English translations. However, the choices of data used within this research study have been greatly influenced by the availability of public documents, but there were no issues encountered with regards to the language barrier as the legal documents that were made public on the archival site were all in English.

In addition, the use of thematic analysis also had its own limitation as a data analysis method which has been partially mitigated by the use of the case study design. Thematic analysis allows room for the researcher to get lost in the content of the data or materials, especially in an exploratory study, which can either detract the

researcher from the research aims and objectives, or it can make the researcher too focused on certain themes and elements; thus, negating the potentially new discovery that could be made from the textual dataset. The case study design helped to mitigate this by narrowing down the scope of the study to within a timeframe and focusing on specific subject matter, which allowed for a more focused approach in investigating, coding, and interpreting the data.

4. Recommendations for future studies

This research study is exploratory in nature that primarily examined the case of doxing in Hong Kong through specifically looking at the 2021 Amendment that was introduced as a response to combat doxing. The findings of this research study provided insights as to the legal measures that have been introduced to address doxing, as well as provided insights as to the doxing problem in Hong Kong before these measures were introduced and how the HKPCPD has responded in light of the 2021 Amendment. This research study serves only as a preliminary exploration and analysis of the legal measures taken in Hong Kong. Hence, the findings are important in providing contextual information and insights on doxing in Hong Kong, as well as insights as to the specifics of the legal measures that were introduced as well as how the law enforcement operated under these changes. They also serve as a basis to branch into more future studies.

Given the observed challenges and responses by law enforcement in this study, it is crucial to conduct more studies to further investigate this practice, as well as to further inform the literature on this subject. This research study only observed the data on the changes introduced in the legislation and the data reported on law enforcement's response after the 2021 Amendment came into effect. Further studies into the actual effects of the implementations of this 2021 Amendment should be considered, especially after there has been a long enough time from the effective date of the amendment in order for more data to be available. Moreover,

this research study purely examined what has been officially reported by the public documents and by the HKPCPD. Further studies can potentially look into data on how the 2021 Amendment has affected the public's experience with doxing. Alternately, further studies can also examine how doxing cases have been addressed differently in court after the 2021 Amendment.

5. Conclusion

In summary, this research study was conducted with the aims of investigating and examining doxing and the effects it has in the context of Hong Kong, as well as investigating and understanding how doxing is legally addressed in the context of Hong Kong. Three research questions were raised, and in answering these questions, seven relevant key findings were found. The first question concerns the challenges posed by doxing to Hong Kong law enforcement before legal measures were introduced to address the practice. Three relevant key findings answer to this question which laid out the challenges that the HKPCPD faced in responding to doxing cases before the 2021 Amendment came into effect. The second question concerns the legal measures introduced in the 2021 Amendment. This research study found that the legal measures were introduced based on three objectives to combat doxing in Hong Kong. The third question concerns how law enforcement responded to doxing after the legal measures were introduced. Three relevant key findings answer to this question which pointed to the differences of how the HKPCPD addressed and handled doxing cases after the legal measures were introduced.

As this research study is exploratory in nature, there are certain limitations which need to be acknowledged with regards to the choices in research design, data selection, and data analysis approach. Despite the limitations, this research study also serves to provide contextual basis on doxing and legal measures to address this in Hong Kong. Further studies on this topic can potentially address the long-term

effects of the 2021 Amendment on doxing in Hong Kong, the Hong Kong people's experience with doxing after the legal measures were introduced, or examining how doxing cases are being addressed in court after the 2021 Amendment came into effect.

Bibliography

Adams, R. & Lytvynenko, J., (2019) Someone Is Doxing Hong Kong Protesters And Journalists — And China Wants Them To Keep Going. [Online] Available at: https://www.buzzfeednews.com/article/rosalindadams/hong-kong-doxing-protesters-china-encourage, [Accessed 2 March 2022].

Anderson, B. & Wood, M. A., (2021) 'Doxxing: A Scoping Review and Typology', In: The Emerald International Handbook of Technology-Facilitated Violence and Abuse. s.l.:Emerald Publishing Limited, p. 205–226.

Anguita, P. R., (2021) 'Freedom of Expression in Social Networks', In: L. Corredoira, I. Bel Mallén & C. Presuel. Rodriogo (eds.) The Handbook of Communication Rights, Law, and Ethics. s.l.:John Wiley & Sons, Inc., pp. 279-291.

Baasanjav, U. B., Fernback, J. & Pan, X., (2019) 'A critical discourse analysis of the human flesh search engine', Media Asia, 46(1-2), pp. 18-34.

Bailey, J., Henry, N. & Flynn, A., (2021) 'Technology-Facilitated Violence and Abuse: International Perspectives and Experiences', In: The Emerald International Handbook of Technology-Facilitated Violence and Abuse. s.l.:Emerald Publishing Limited, pp. 1-17.

Barry, P. B., (2022) '#MeToo and the Ethics of Doxing Sexual Transgressors', In: D. Boonin, (ed.) The Palgrave Handbook of Sexual Ethics. Boulder, CO: Palgrave Macmillian, pp. 507-523.

Cambridge Dictionary, (2022) *doxing.* [Online] Available at: https://dictionary.cambridge.org/dictionary/english/doxing [Accessed 21 March 2022].

Chang, L. Y., (2020) ‘Taking justice into their own hands: 'Netilantism in Hong Kong'’, In: J. Golley, L. Jaivin, B. Hillman & S. Strange, (eds.) China Story Yearbook: China Dreams. s.l.:s.n., pp. 217-219.

Chen, M., Cheung, A. S. Y. & Chan, K. L., (2019) ‘Doxing: What Adolescents Look for and Their Intentions’, Internation Journal of Environmental Research and Public Health, Volume 16, Number 218, pp. 1-14.

Cheung, A., (2021) ‘Doxing and the Challenge to Legal Regulataion: When Personal Data Become a Weapon’, In: The Emerald International Handbook of Technology-Facilitated Violence and Abuse. s.l.: Emerald Publishing Limited, p. 577–594.

Chia, S. C., (2019) ‘Crowd-sourcing justice: tracking a decade's news coverage of cyber vigilantism throughout the Greater China region’, Information, Communication & Society, Volume 22, Number 14, pp. 2045-2062.

Clarke, V. & Braun, V., (2017) ‘Thematic analysis’, The Journal of Positive Psychology, Volume 12, Number 3, pp. 1-2.

Creswell, J. W. & Creswell, J. D., (2018) Research Design Qualitative, Quantitative, and Mixed Methods Approaches Fifth Edition. Los Angeles: SAGE Publications, Inc..

Creswell, J. W. & Poth, C. N., (2018) Qualitative Inquiry & Research Design Choosing from Among Five Approaches Fourth Edition. Los Angeles: SAGE Publications, Inc..

Douglas, D. M., (2016) ‘Doxing: a conceptual analysis’, Ethics and Information Technology, Volume 18, pp. 199-210.

e Silva, K. K., (2018) ‘Vigilantism and cooperative criminal justice: is there a place for cybersecurity vigilantes in cybercrime fighting?’, International

Review of Law, Computers & Technology, Volume 32, Number 1, pp. 21-36.

Favarel-Garrigues, G., Tanner, S. & Trottier, D., (2020) 'Introducing digital vigilantism', Global Crime, Volume 21, Number 3-4, pp. 189-195.

Fish, A. & Follis, L., (2016) 'Gagged and Doxed: Hacktivism's Self-Incrimination Complex', International Journal of Communication, Volume 10, p. 3281–3300.

Gao, L. & Stanyer, J., (2014) 'Hunting corrupt officials online: the human flesh search engine and the search for justice in China', Information, Communication & Society, Volume 17, Number 7, pp. 814-829.

Gonella, N. & Nericcio, L., (2017) 'On Ethics and Doxing', Cybersecurity Case Library, Volume 1, Number 1, pp. 28-37.

Hale, E., (2019) Hong Kong protests: tech war opens up with doxxing of protesters and police. [Online] Available at: https://www.theguardian.com/world/2019/sep/20/hong-kong-protests-tech-war-opens-up-with-doxxing-of-protesters-and-police, [Accessed 2 March 2022].

Han, D., (2018) 'Search boundaries: human flesh search, privacy law, and internet regulation in China', Asian Journal of Communication, Volume 28, Number 4, pp. 434-447.

HKPCPD, Privacy Commissioner for Personal Data, (2020) Rising to the Novel Challenges: 2019-20 Annual Report, Hong Kong: Privacy Commissioner for Personal Data.

HKPCPD, Privacy Commissioner for Personal Data, (2021) Guardian Privacy 25 Years: 2020-21 Annual Report, Hong Kong: Privacy Commissioner for Personal Data.

HKPCPD, Privacy Commissioner for Personal Data, (2021) Survey of Public Attitudes on Personal Data Privacy Protection 2020, Hong Kong: Privacy Commissioner for Personal Data.

HKPCPD, Privacy Commissioner for Personal Data, (2022) A New Era in the Regulatory Regime for the Protection of Personal Data: 2021-22 Annual Report, Hong Kong: Privacy Commissioner for Personal Data.

Huang, Q., (2021) 'The mediated and mediatised justice-seeking: Chinese digital vigilantism from 2006 to 2018', Internet Histories, Volume 5, Number 3-4, pp. 304-322.

Kiger, M. E. & Varpio, L., (2020) 'Thematic analysis of qualitative data: AMEE Guide No. 131', Medical Teacher, pp. 1-9.

Lee, C., (2022) 'Doxxing as discursive action in a social movement', Critical Discourse Studies, Volume 19, Number 3, pp. 326-344.

Loveluck, B., (2020) 'The many shades of digital vigilantism. A typology of online self-justice', Global Crime, Volume 21, Number 3-4, pp. 213-241.

MacAllister, J. M., (2017) 'The Doxing Dilemma: Seeking a remedy for the malicious publication of personal information', Fordham Law Review, Volume 85, Number 5, pp. 2451-2484 .

Makinde, O. A. et al., (2021) 'The Nature of Technology-Facilitated Violence and Abuse among Young Adults in Sub-Saharan Africa', In: The Emerald International Handbook of Technology-Facilitated Violence and Abuse. s.l.:Emerald Publishing Limited, p. 83–101.

Privacy Commisioner for Personal Data HKPCPD, (2022), Doxxing Offences. [Online] Available at: <https://www.pcpd.org.hk/english/doxxing/index.html> , [Accessed January 2022].

Oxford Reference, (2022) *doxing.* [Online], Available at: https://www.oxfordreference.com/view/10.1093/acref/9780191803093.001.0001/acref-9780191803093-e-405, [Accessed 22 March 2022].

Pacheco, E. & Melhuish, N., (2021) 'The Face of Technology-Facilitated Aggression in New Zealand: Exploring Adult Aggressors' Behaviors', In: The Emerald International Handbook of Technology-Facilitated Violence and Abuse. s.l.:Emerald Publishing Limited.

Personal Data (Privacy) Ordinance (Cap. 486) (1996).

Personal Data (Privacy) Ordinance (Cap. 486) (2021).

Personal Data (Privacy) Ordinance (Cap.486) (2012).

Purbrick, M., (2019) 'A Report of the 2019 Hong Kong Protests', Asian Affairs, Volume 50 Number 4, pp. 465-487.

Silva Martins, F., Carneiro da Cunha, J. & Fernando, S., (2018) 'Secondary Data in Research - Use and Opportunities', Revista Ibero-Americana de Estrategia, Volume 17, pp. 1-4.

Smallridge, J. & Wagner, P., (2019) 'The Rise of Online Vigilantism',. In: T. J. Holt & A. M. Bossler, (eds.) The Palgrave Handbook of International Cybercrime and Cyberdeviance. Cham: Palgrave Macmillan, pp. 1307-1331.

Snyder, P., Doerfler, P., Kanich, C. & McCoy, D., (2017) Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing. London, Association for Computing Machinery.

Trottier, D., (2020). 'Denunciation and doxing: towards a conceptual model of digital vigilantism', Global Crime, Volume 2, Number 3-4, pp. 196-212.

Tsui, L., (2020) ' Doxxing and press freedom in Hong Kong', Media Asia, Volume 47, Number 3-4, pp. 172-173.

Zainal, Z., (2007) '*Case study as a research method', Jurnal Kemanusiaan,* Volume 9, pp. 1-6.