Chapter 34

Doxing and the Challenge to Legal Regulation: When Personal Data Become a Weapon

Anne Cheung

Abstract

Doxing refers to the intentional public release by a third party of personal data without consent, often with the intent to humiliate, intimidate, harass, or punish the individual concerned. Intuitively, it is tempting to condemn doxing as a crude form of cyber violence that weaponizes personal data. When it is used as a strategy of resistance by the powerless to hold the powerful accountable, however, a more nuanced understanding is called for. This chapter focuses on the doxing phenomenon in Hong Kong, where doxing incidents against police officers and their family members have skyrocketed since 2019 (a 75-fold increase over 2018). It contends that doxing for political purposes is closely related to digital vigilantism, signifying a loss of confidence in the ruling authority and a yearning for an alternative form of justice. The chapter therefore argues that public interest should be recognized as a legal defense in doxing cases when those discharging or entrusted with public duty are the targets. Equally, it is important to confine the categories of personal data disclosed to information necessary to reveal the alleged wrongdoer or wrongdoing. Only in this way can a fair balance be struck between privacy, freedom of expression, and public interest.

Keywords: Doxing; injunction; privacy; public interest; personal data; Hong Kong

The Emerald International Handbook of Technology-Facilitated Violence and Abuse, 577–594

doi:10.1108/978-1-83982-848-520211041

Introduction

It is often said that personal data are the new oil and currency of modern economies (The Economist, 2017). However, personal data can also become a digital weapon, as evidenced by the phenomenon of doxing, which can easily escalate into Technology-Facilitated harassment. Doxing is generally defined as the intentional public release on the internet of personal data that can be used to identify or locate an individual without their consent. It is often done with the intent to humiliate, threaten, intimidate, or punish the identified individual (Douglas, 2016, p. 199). Once personal data have been released on and circulated via the internet, they are extremely difficult to erase. This "low-tech, high-harm" form of privacy violation often brings about immense disruption and anxiety, and sometimes even the risk of physical harm or other grave consequences (NYU Tandon School of Engineering, 2017, para 1). There are thus pressing calls for legal intervention and regulation.

On its face, there seem to be overwhelming reasons to denounce doxing completely as a toxic practice and a form of Technology-Facilitated violence and abuse (TFVA). Although it undoubtedly has a dark side, doxing – or the unauthorized disclosure of personal data – has also become an important tactic for those engaged in social action. For example, netizens used doxing to expose the identity of police officers who had allegedly used excessive force against peaceful demonstrators during Occupy Wall Street (Tenold, 2018), and the hacker group known as Anonymous released the personal data of KKK members as part of the fight against racism (Woolf, 2015). Doxing is seen by some as the "democratization of force," a resistance tactic, and a political tool to expose and shame wrongdoers (Tenold, 2018, para 14). Trottier (2019) observed that doxing for political purposes is closely affiliated with the notion of digital vigilantism, that is, netizens taking the law into their own hands in the name of justice.

This chapter focuses on doxing as a tactic of political action and resistance, arguing that doxing to increase the transparency of the government or to bring to light newsworthy information of public interest serves an important checks and balances function in society, especially in political contexts where public power is widely perceived to have gone awry (Trottier, 2019, p. 6). Situated in the context of ongoing protests in Hong Kong, which kicked off in June 2019, the chapter advocates for a more nuanced approach to doxing, taking the position that doxing that serves the primary aim of deanonymizing those discharging or entrusted with public duty to establish their identity and hold them accountable for their wrongdoing, warrants different considerations from doxing in other contexts. Provided that the personal data disclosed in these kinds of circumstances are confined to the information necessary to reveal the alleged wrongdoers or their wrongdoing, without releasing personal data of family members, a public interest defense should be available.

This chapter uses Hong Kong as a case study to examine doxing, not as a general phenomenon, but as a specific form of calling public officials to account for their alleged wrongdoing. It first discusses literature relating to doxing in the pursuit of justice. Next, it provides background about the context in which doxing has occurred in Hong Kong. It then turns to consider the ways in which doxing was raised in three cases before the Hong Kong Court, analyzing the significance

in each case by examining who applied for injunctive relief, against whom the order was granted, and the scope of the order granted. Finding that the Court overreached, the chapter then focuses on articulating the justification for and parameters of a proposed public interest defense that would allow for a better balancing of the competing interests at stake when doxing is used to call public officials to account. It concludes by recognizing that, although doxing can be a form of TFVA, there may be limited contexts in which its use can be justified.

Doxing and the Pursuit of Justice

"Doxing" (or sometimes "doxxing") comes from an alternative spelling of the abbreviation of documents, i.e., "docs," prevalent in the hacker world. It originally referred to documenting, compiling, uncovering, and/or releasing personal data on an individual or group on the internet. The term was first used in the 1990s in the context of hackers doxing a rival hacker (Cooper, 2019). Over the years, doxing has evolved into a practice that a group of netizens engages in in a coordinated or spontaneous manner. It often takes the form of the crowdsourcing of information, with available personal data gathered and published by a number of netizens, resulting in a "dossier" on the targeted individuals. When netizens mobilize to cyber-hunt perceived wrongdoers, a vast amount of personal data is exposed, which can easily escalate into harassment, sometimes of innocent parties, as seen in the aftermath of the Boston Marathon bombing in 2013 when a university student who had been wrongly identified by netizens as a culprit was harassed and committed suicide shortly after being doxed (Lee, 2013).

In a study of over 5,500 online text files associated with doxing, a group of US scholars found that more than 90% included the victim's address, 61% included a phone number, 53% included an e-mail address, and 51% included information on family members (Snyder, Doerfler, Kanich, & McCoy, 2017). When such identifying information is disclosed, doxing can easily lead to in-person harassment, stalking, and vilification. Despite the negative connotations of doxing, the same study showed the most common reason for doxing to be seeking justice against something that was seen to be immoral or unfair to a third party (68%), with doxing targets including both individuals who had allegedly cheated others in online forums and law enforcement officers (Snyder et al., 2017).

In fact, malicious intent is not a prerequisite for doxing. Often, doxing is used as a tool of protest to increase transparency and expose wrongdoing, which is analogous to whistleblowing that reveals wrongdoing within an organization (Douglas, 2016, pp. 200 & 206). Yet, as the exposure is not done by insiders, it makes sense for MacAllister (2017) to characterize the act as "doxing for political purposes" (p. 2454) to mark its distinction from doxing for purely malicious purposes such as revenge, harassment, or stalking. Trottier (2019) further identifies doxing as a form of digital vigilantism whereby individuals aim to achieve justice by relying on digital media to denounce and shame those deemed to have transgressed legal or moral boundaries. Nevertheless, it is a form of private justice that is both extra-state and extra-legal (Trottier, 2017, p. 61). Trottier (2017)

warns that digital vigilantism not only renders a targeted individual visible and subject to monitoring; it is often a sign that the public is losing confidence in the state's ability to manage crime and losing faith in the police and criminal justice (p. 62). It may even foreshadow a crisis of legitimacy in the state.

Doxing in the Context of Hong Kong Protests

Hong Kong provides fertile ground for digital vigilantism: since June 2019, public confidence in the police has reached an all-time low, and the city has been wracked by political protests that saw hundreds marching in the streets and multiple incidents of police violence (CNN, 2020). The turmoil was initially sparked by a proposed extradition bill that would have allowed criminal suspects to be extradited to mainland China under certain circumstances, triggering fears that anyone present in Hong Kong would be at risk of an unfair trial or even violent treatment in the mainland (BBC News, 2019; see also Fugitive Offenders and Mutual Legal Assistance in Criminal Matters Legislation (Amendment) Bill, 2019). Numerous rounds of protest have seen tear gas, plastic bullets, and water cannons wielded against protestors by the police (Amnesty International, 2019a), with a journalist and a voluntary health worker left partially blinded after being hit in the eye by police projectiles (Graham-Harrison, Kuo, & Yu, 2019; Kilpatrick, 2019). In another incident, a teenage protestor was shot in the chest at close range (Graham-Harrison et al., 2019), and there are many reports of the police resorting to arbitrary arrests and unnecessary violence against protesters (Amnesty International, 2019b). In a public opinion poll conducted in October 2019, nearly 70% of the more than 800 respondents were in favor of restructuring the police force, and over half gave the police a grade of zero (Lee, 2019). For their part, protestors have also escalated the violence, hurling bricks and petrol bombs at police officers and police stations (Lo & Mok, 2020).

As the city has been dragged deeper and deeper into political conflict, doxing is increasingly being used as a tactic, largely against police officers alleged to have engaged in abusive tactics (Privacy Commissioner for Personal Data, Hong Kong [PCPD], 2020a), although journalists and protesters critical of government and law enforcement policies and tactics have also been targeted (Chan & Blundy, 2019).

According to the Office of the PCPD (2020a), there were 4,400 doxing-related complaints between June 14, 2019 and January 10, 2020, involving 17 online social media platforms and nearly 3,000 web links, which represents a 75-fold increase over 2018.[1] Of the 4,400 complaints, 36% concerned police officers or their family members, 4% concerned government officials or public servants, 30% concerned members of the public who had expressed views in support of the government or the police, 10% concerned citizens who had made online comments against the government or police, and 20% concerned protestors. During this period, eight people have thus far been arrested for contravening section 64(2) of the Personal Data Privacy Ordinance in disclosing any personal data about another individual without their consent and if the disclosure causes psychological harm (PCPD, 2020a). In November 2020, a telecommunication technician became the first person to be convicted of doxing – violating section 64(2) of the PDPO – for obtaining and disclosing the personal data of police officers and their

family members without consent (*HKSAR v Chan King Hei* (2020)). The defendant was sentenced to imprisonment for 18 months (PCPD, 2020b).

Doxing of the police is believed to have begun after police officers stopped displaying identifying badge numbers on their uniforms while dealing with the protests (Hale, 2019), prompting protesters to attempt to identify the individual officers concerned through other means, including doxing, which soon extended to officers' family members. It is not only the police who have been targeted. Journalists and protesters have also been doxed by the pro-authorities camp (Hale, 2019). In one instance, police officers went so far as to hold up the identity cards and press passes of journalists in front of a live-streaming camera during a stop and search operation (Leung, 2020). The doxing perpetrated by the pro-authorities camp is also apparently much more organized than that by protestors. For example, a site called HK Leaks, which targets pro-democracy leaders, protesters, and journalists, is registered anonymously on a Russian server and is promoted by powerful groups with links to China's ruling Communist Party (Chan & Blundy, 2019).

Doxing engaged in by the opposing sides has turned the internet into a new and dramatic form of political theater played out for all to see, opening up new mobilizing strategies for participants at both ends of the political spectrum (Lustbader & Gullapalli, 2019). Although doxing has been used as a tool by both the antigovernment and pro-authorities camps, the nature of that use is very different. Doxing by the former constitutes a citizen-led intervention, largely against the police and government officials. It is an attempt by the powerless to voice their disapproval of the actions of the powerful, to police the police whose power has gone unchecked. Like the military, the police force is a state institution that has monopolized the legitimate use of violence. Lashing out against the police represents anger, dissatisfaction, and frustration with asymmetrical power relations and abuses of power. Moreover, as representatives of the state authority, the police have borne the brunt of public anger in demonstrations against the extradition bill and during the long fight for democracy in Hong Kong. From this perspective, doxing is closely affiliated with digital vigilantism, a form of collective digital resistance, which appeals to the established norm of holding authorities accountable. The presumed connection between the pro-authorities camp and the state, in contrast, has rendered doxing by the former a weapon for silencing dissenting voices, and the death threats against journalists uttered on the sites an ugly means of intimidation. Further, in using doxing as a tactic against protesters, the pro-authorities camp has illustrated that doxing for political purposes is no longer a tool used solely by the self-proclaimed righteous to expose wrongdoers; it is a tool that is available to everyone and can be used against anyone. Arguably, in drawing moral equivalence between doxing as a powerful tool in the fight for democracy and doxing as a potent weapon for punishing troublemakers, the pro-authorities camp has reminded us of the repugnant nature of doxing and stopped ethical protesters from celebrating its use. In other words, doxing has been used as a tool of the powerful and its capacity for use by the powerless has been limited.

Doxing, in the context of social action, invokes the complex dynamics of social power and the exercise of free speech, as well as the differing responsibilities of

individuals and the government. Not only has personal data become weaponized, but the "weaponized visibility" of targeted victims has emerged as an object for monitoring and control (Trottier, 2017, pp. 65–66). What remains critical is to determine whether, and if so when, doxing could be justified.

Doxing before the Hong Kong Court

In October 2019, the Hong Kong court finally made its judicial stance on doxing known by granting three interim injunction orders. The first concerned an action brought by *Apple Daily*, a widely circulated local newspaper. The Court granted an interim injunction restraining anyone from disclosing or publishing the personal details of *Apple Daily* staff or helping anyone to do so (HC 1741/2019, cited in *Junior Police Officers' Association*, 2019a, HKCA, para 20). At least 18 of the paper's journalists had been doxed on a Russia-hosted website that sought "to know who these people are and why [they are] messing up Hong Kong" (Lau & Ng, 2019). As a written judgment is not available for this case, analysis of judicial reasoning related to doxing can only be carried out for the two other injunction cases.

The second doxing case was brought by the Junior Police Officers' Association and heard by the Hong Kong Court of Appeal (HKCA) (2019a). In *Junior Police Officers' Association of the Hong Kong Police Force v Electoral Affairs Commission and others* (2019a) (the decision on substantive merits of the case was later heard and will be referred as *Junior Police Officers' Association*, 2020a),[2] the HKCA overturned a lower court ruling and granted an interim injunction prohibiting the electoral registers showing the names of the registered electors together with their principal residential address (i.e., the linked information) in the district council polls in November 2019. The challenge was based on the rights to privacy under article 14 of the Hong Kong Bill of Rights (HKBOR) and the right to vote under article 26 of the Basic Law. The court emphasized that it is only the disclosure of that linked information, which would facilitate the doxing of police officers' family members, that was being restricted and further noted that more than 2,000 police officers and family members had been subject to doxing between June and October 2019 (*Junior Police Officers' Association*, 2019a, HKCA, paras 3–4 & 51). The HKCA defined "doxing" as the "extensive leaking of personal information and cyberbullying on the internet and various social and other media" (*Junior Police Officers' Association*, 2019a, para 4).

In dealing with interim injunctions in public law, the Hong Kong court generally applies the well-established principles governing civil cases laid down in the English landmark case of *American Cyanamid Co. (No. 1) v Ethicon Ltd.* (1975),[3] albeit with certain necessary modifications (*Junior Police Officers' Association*, 2019a, HKCA, para 14).[4] One main modification pertains to the question of balance of convenience,[5] with the Hong Kong court adopting a wider view than just the interests of the immediate parties to the application to take the public interest into account. First, the HKCA took the view that the interests of the great majority of the police force (85% of which the plaintiff represented) were at stake (*Junior Police Officers' Association*, 2019a). There was cogent evidence to

show that police officers and their families had been subjected to doxing, accompanied by harassment, intimidation, and serious threats against personal safety (*Junior Police Officers' Association*, 2019a, HKCA, para 18). The HKCA condemned doxing as a "hideous practice, as [a] weapon to cause harm to individuals and target groups" (*Junior Police Officers' Association*, 2019a, para 19). The Court considered that the possibility of identifying a police officer's residential address through the register's list was not a "fanciful risk" (*Junior Police Officers' Association*, 2019a, HKCA, para 31). Second, the Court further stated doxing seriously endangers our society as a whole for it will instill a chilling effect on our society when many are intimidated into silence for fear of being victimized by doxing (*Junior Police Officers' Association*, 2019a, HKCA). Third, with respect to the issue of balance, the HKCA's decision is grounded in the protection of privacy, although the court did not go into detail concerning the nature and scope of the privacy interest involved (*Junior Police Officers' Association*, 2019a). Finally, the court ruled that there was a wider public interest at stake in safeguarding the integrity of the then upcoming district council election. In an attempt to strike a balance between privacy and public access to the Final Register, the HKCA decided to allow only validly nominated candidates and their political parties to have access to the linked information therein (*Junior Police Officers' Association*, 2019a, para 51).

The third relevant application for an interim injunction was in *Secretary for Justice and Commissioner of Police v Persons Unlawfully and Wilfully Conducting Themselves in any of the Acts Prohibited under Paragraph 1(a), (b) or (c) of the Indorsement of Claim* (2019a) (hereinafter referred as *Secretary for Justice and Commissioner of Police*).[6] Justice Chow of the Hong Kong Court of First Instance (HKCFI) granted the interim injunction that prohibited "using, publishing, communicating or disclosing to any other person the personal data" of any police officers and/or their family members intended or likely to intimidate, molest, harass, threaten, pester, or interfere with them (*Secretary for Justice and Commissioner of Police*, 2019a, para 1).[7] Personal data included but were not limited to the name, job title, residential address, office address, school address, e-mail address, date of birth, telephone number, identity card number or identification number on any official identity document, Facebook account ID, and license plate number of any police officer and/or their family members, as well as photographs thereof. The application of the continuation of the interim injunction was later heard and granted by Justice Coleman, who added a journalism exemption to balance government accountability, privacy, and freedom of the press (*Secretary for Justice and Commissioner of Police*, 2019b). This was in response to the Hong Kong Journalists Association's application for the order to be varied to exclude "news activity" from the prohibition. As the reasoning behind Justice Chow's initial granting of the interim injunction is unavailable, we focus here on the judgment delivered by Justice Coleman.[8]

Justice Coleman first ruled that the applicant had demonstrated that what the defendant did was threatening, and in fact intended, to cause imminent and substantial harm. He then stated that he was satisfied that widespread doxing activities had created a state of affairs in society that endangered the lives, safety,

health, property, or comfort of the public, which constituted a public nuisance (*Secretary for Justice and Commissioner of Police,* 2019b, para 39). In addition, doxing activities and the resulting harassment and intimidation had caused intimidation or fear of harm (*Secretary for Justice and Commissioner of Police,* 2019b, para 40). Further, the damage caused by public nuisance and intimidation was not quantifiable, and an award of damages could not be an adequate remedy (*Secretary for Justice and Commissioner of Police,* 2019b, para 41). Finally, as to the test of balance of convenience, Justice Coleman concluded that it was strongly in favor of granting the injunction (*Secretary for Justice and Commissioner of Police,* 2019b, para 45). In weighing the different interests at stake, he acknowledged that the right to freedom of expression had to be considered together with the rights of police officers and their family members to respect and privacy, and with the need to maintain public order (*Secretary for Justice and Commissioner of Police,* 2019b, para 43). On balance, he was prepared to amend the injunction order to exclude news activity, as it was never the court's intention to "stifle genuine and lawful journalistic activities" (*Secretary for Justice and Commissioner of Police,* 2019b, para 68). In summary, "real journalists" would be entitled to report personal information about police officers in order to carry out the valuable watchdog role of the press, but "fake journalists" whose activities amounted to nuisance, harassment, or intimidation would not and should be punished for doing so (*Secretary for Justice and Commissioner of Police,* 2019b, paras 68–70).

At this point, it is worth examining the three court decisions by probing three queries: who applied for the interim injunction order concerned; against whom was the order granted; and what was the order's scope? The answers to these questions enable us to better understand the dynamics of doxing in a political context when the authorities have resorted to legislative measures to suppress attempts to call for accountability. It also lends support to the need for a public interest defense to the offense of doxing.

Who Applied for the Interim Injunction?

An application for the granting of an injunction order can be filed by any party. In the three aforementioned decisions, the applications were made by a newspaper to protect its journalists, by the Junior Police Officers' Association on behalf of the majority of the Hong Kong Police Force, by the Commissioner of Police on his own behalf and that of all police officers, and by the Secretary for Justice on behalf of the public at large. In this battle over doxing, it is obvious what interests the first three applicants represented and what parties they wished to protect. However, the interests pursued by the Secretary for Justice and the role that she played were not entirely clear or convincing. In other words, who constituted the public at large and whose interests was the Secretary seeking to protect?

In *Secretary for Justice and Commissioner of Police* (2019b), Justice Coleman noted that the Secretary for Justice had brought the application in her role as "guardian of the public" (para 26). He also acknowledged that many would "see some irony in the invocation of that role," and question whether the Secretary for

Justice was in fact "protecting only, or primarily, police officers and their families" (*Secretary for Justice and Commissioner of Police,* 2019b, para 27). Further, he took judicial notice of the concern raised by a significant number of people that some police officers had failed to protect the public or even on occasion made victims of some members of the public (*Secretary for Justice and Commissioner of Police,* 2019b, para 27). Nevertheless, Justice Coleman was equally quick to add that he could not presume that the Secretary for Justice had not been taking appropriate and necessary follow-up measures concerning allegations of improper conduct, regardless of how slow the process might seem to be (*Secretary for Justice and Commissioner of Police,* 2019b, para 28). In addition, he relied on *Junior Police Officers' Association* (2019a) to emphasize that doxing's effects extend far beyond its immediate targets to exert a harmful effect on society as a whole. Finally, he cautioned that "two wrongs do not make a right," referring directly to the allegation and perception that even if some members of the police force have "conducted themselves in a way which does no credit to the force," doxing can never be justified (*Secretary for Justice and Commissioner of Police,* 2019b, para 32). Overall, Justice Coleman's decision is to be applauded for recognizing the political crisis in which Hong Kong is embroiled and honestly confronting the political overtones of the legal issue he had been asked to resolve (*Secretary for Justice and Commissioner of Police,* 2019b, paras 34–35).

Yet, it is in treading exactly this line of logic that one finds little solace or faith in the Secretary for Justice or even in the Hong Kong court system. Although the doxing and harassment of police officers and their family members (which represent 36% of doxing complaints made to the Privacy Commissioner) have to be condemned, their interests are already represented by the Junior Police Association and the Commissioner of Police. In contrast, the protesters and members of the public who have been doxed for expressing views critical of the police and government (30% of total doxing complaints) (PCPD, 2020a) have no representation. The powerless have no means or knowledge to start legal proceedings. Sadly, as custodian of the public interest, the Secretary for Justice has chosen only to side with the police force as the injunction order was effective only to protect the police officers and their family members. In parallel, while recognizing the frustration of the public, a high court judge asked the public to be patient and to put up with the allegedly nonprofessional conduct of the police until a better solution can be devised.

Against Whom was the Order Granted?

Of the three decisions discussed, only the second named a specific defendant, namely, the Electoral Affairs Commission (and others). The other two decisions were, in effect, being brought against anyone anywhere in the world. Justice Coleman remarked that the identification of defendants on a writ or injunction order without naming any individual had been approved in previous cases (*Secretary for Justice and Commissioner of Police,* 2019b, para 7). He further noted that while it is a fundamental principle of justice to ensure that a person is not

made subject to the jurisdiction of the court without having such notice of proceedings as would enable them to be heard, he was satisfied that the description adopted to identify the defendant had met this requirement, as the mode of service could reasonably give rise to an expectation that the proceedings would come to the relevant person's attention (*Secretary for Justice and Commissioner of Police,* 2019b, para 7).

Justice Coleman's reasoning was unfortunately made without any reference, and is in direct contradiction, to the UK Supreme Court's decision in *Cameron v Liverpool Victoria Insurance* (2019), which is of high persuasive value.[9] Here, the Supreme Court's reasoning on the requirements of justice is of particular pertinence to the issue of injunction orders against unnamed parties.

The plaintiff in *Cameron v Liverpool Victoria Insurance* (2019) had been injured in a car accident caused by a hit-and-run driver who could not be identified. The issue at stake was whether legal action can be brought against an unnamed and unidentifiable defendant (*Cameron v Liverpool Victoria Insurance*, 2019, paras 1 & 12). In delivering the leading judgment of a unanimous court, Lord Sumption gave a definitively negative answer and overruled previous judgments that allowed such a practice (*Cameron v Liverpool Victoria Insurance*, 2019, para 21). Although he admitted that English law has permitted actions, including injunctions, against unnamed wrongdoers, with specific reference to such jurisdiction being regularly invoked in the context of abuse of the internet, "the powerful tool for anonymous wrongdoing," Lord Sumption drew a distinction between two categories of unnamed defendants (*Cameron v Liverpool Victoria Insurance*, 2019, para 11). The first category comprises anonymous defendants who are identifiable but whose names are unknown, such as squatters occupying a property who are identifiable by their location, whereas the second comprises defendants who are not only anonymous but cannot be identified. In the first category, the defendant is described in a way that makes it possible in principle to locate or communicate with him or her and to determine without further inquiry whether he or she is the person described in the claim form, whereas in the second category they are not described in an identifiable manner (*Cameron v Liverpool Victoria Insurance*, 2019, para 13). Lord Sumption pointed out that the fundamental principle of natural justice requires that a court give a litigant notice of the proceedings against them to enable the litigant to be heard (*Cameron v Liverpool Victoria Insurance*, 2019, para 17). In Lord Sumption's opinion, giving notice is vital to determine the balance of rights between the litigants, and afford them an opportunity to substantially present their case before the court (*Cameron v Liverpool Victoria Insurance*, 2019, para 17). He emphasized that effective notice must be served to bring the proceedings to the attention of the defendant, which was the long-standing practice of common law courts before statutory rules of procedure were introduced, and one of the foundations of English litigation procedure for centuries (*Cameron v Liverpool Victoria Insurance*, 2019, paras 18 & 21). Accordingly, Lord Sumption considered previous judgments allowing unnamed and unidentifiable defendants to be sued to be unequivocally wrong (*Cameron v Liverpool Victoria Insurance*, 2019, para 21).

Lord Sumption explained that an unknown person cannot be identified "simply by referring to something that he has done in the past," and thus naming the defendant as a person driving a vehicle that collided with another vehicle on a particular date does not identify anyone (*Cameron v Liverpool Victoria Insurance*, 2019, para 16). He added that although the publicity attending to such proceedings sometimes makes it possible to speculate that the wrongdoer knows about the proceedings, service is an act of the court, and it "cannot be enough that the wrongdoer himself knows who he is" (*Cameron v Liverpool Victoria Insurance*, 2019, para 16). These legal principles are equally applicable to the Hong Kong context.

First, the great emphasis that *Cameron v Liverpool Victoria Insurance* (2019) places on the natural justice principle may well cast doubt on the recent, and increasingly common, practice in Hong Kong of naming unknown defendants by way of a description of their conduct. Doubt may also arise over whether the Hong Kong court had the jurisdiction to grant the recent injunction orders prohibiting doxing against unnamed and unidentifiable defendants by way of a general description of their past or even future conduct, a description that could actually be applicable to the public at large. Allowing such defendants to be sued violates the principle that justice in legal proceedings must be available to both sides (*Cameron v Liverpool Victoria Insurance*, 2019, para 17). Second, in describing the defendants as "[p]ersons unlawfully and wilfully conducting themselves in any of the acts prohibited" under the injunction order (*Secretary for Justice and Commissioner of Police*, 2019b), the HKCFI risked covering persons who had perpetrated no such acts in the past, and so would have no interest in opposing the injunction application, thereby rendering them liable for contempt of court for acts performed in the future. This broad attempt to capture "any" potential defendant amounts to the court making a new law applicable to the public at large that prohibits the doxing of police officers and their family members. Finally, in addition to trespassing the legislative role, it is also doubtful whether the HKCFI has struck the right balance between the various rights involved without the benefit of public consultation and the meticulous law drafting procedures associated with legislation. As injunction orders are granted in civil cases, and thus any breach thereof can be enforced only at the instigation of the plaintiff, the HKCFI's decision risks allowing plaintiffs unchecked discretion to engage in selective enforcement of said legislation.

What was the Scope of the Order Granted?

Doxing involves a direct conflict between one person's freedom of expression and another's right to privacy, both of which are constitutionally protected in Hong Kong.[10] To resolve the conflict, the court has to strike a balance between the two rights, which calls for an examination of the nature of personal data.

In the action brought by *Apple Daily*, the HKCFI prohibited the disclosure of personal details on the 18 journalists concerned. In a similar vein, in *Secretary for Justice and Commissioner of Police* (2019a, 2019b), the HKCFI prohibited the disclosure of *any* personal data on *any* police officers or their family members that was intended or likely to intimidate, molest, harass, threaten, or pester them

(emphasis added). As noted above, the personal data concerned were expansive, including even job titles and e-mail addresses. In marked contrast, the subject matter of the injunction order in *Junior Police Officers' Association* (2019a) is much narrower: the public still has access to the names of registered electors and their principal residential addresses as separate data, rather than as linked-up data (HKCA, para 46). The HKCA was concerned that linked information could be misused for doxing and could have a chilling or deterrent effect such that some individuals would be reluctant to register as electors to exercise their right to vote (*Junior Police Officers' Association*, 2019a, para 53).

Location data, one's home address in particular, are undeniably private. Knowing a targeted person's address allows others to encounter them in person and observe their target's movements, habits, physical appearance, and characteristics (Douglas, 2016). Still, to safeguard the integrity of the then imminent district council election, and to ensure an open, fair, and honest election, the linked information concerned would remain available to all validly nominated candidates and their political parties (*Junior Police Officers' Association*, 2019a, HKCA, paras 33 & 40). The HKCA's approach was consistent with and in direct correlation with its definition of doxing, that is, the extensive leaking of personal information *and* cyberbullying on the internet and various social and other media (emphasis added) (*Junior Police Officers' Association* 2019a, para 4). There must be a close connection between the type of personal data leaked and the subsequent forms of misuse and harm, constituting "the worst and [most] reprehensible forms of intrusion of the privacy of the individuals concerned" (*Junior Police Officers' Association*, 2019a, HKCA, para 18).

Shortly after delivering the interim injunction order, the HKCA was asked to rule on the substantive merits of the same case in *Junior Police Officers' Association* (2020a). The issue concerns whether making available the linked information for public inspection would have violated the registered voters' right to privacy and the right to vote. The HKCA reiterated that a fair balance has to be struck between the voters' rights and societal benefit of making known the linked information (*Junior Police Officers' Association*, 2020a). It ruled that the injunction order has to be relaxed to allow candidates, the press, and political parties to have access to the linked information (*Junior Police Officers' Association*, 2020a, HKCA, para 104). At the same time, the electoral authorities should have limited discretion to restrict inspection of the linked information for those voters who have valid safety concerns (*Junior Police Officers' Association*, 2020a, para 108). Substantive hearing of the case also reveals the limitations of an interim injunction application where merits of substantive arguments cannot be fully articulated, resulting in premature and unjustified curtailment of rights of the parties.

In comparison, the other two judgments – *Apple Daily* and *Secretary for Justice and Commissioner of Police* (2019a, 2019b) – are hearings on interim injunction applications without any follow-up hearings on the substantive merits of the case (given the absence of the unnamed defendants). The interim injunction orders granted were broad and vague in terms of the personal data covered. Both orders covered the names, job titles, and office addresses of the protected class of persons in question. Although Justice Coleman in the latter case referred explicitly to the

need to balance freedom of expression with the right to privacy (*Secretary for Justice and Commissioner of Police,* 2019b, paras 31, 43, & 44), he did not examine the nature of the personal data involved. He made no attempt to explain why names, job titles, and office addresses, particularly those of police officers, who should be accountable to the public, should not be disclosed. While it is only fair and just that the personal data of their family members should not be disclosed without consent, for they are unrelated to the exercise of public duty, the court's prohibition on the disclosure of any personal data on police officers is questionable indeed. Although the injunction order specifies that it is disclosure coupled with an intention to intimidate, molest, harass, threaten, or pester – or the likelihood of intimidation, molestation, harassment, threats, or pestering occurring – that is objectionable, a number of uncertainties remain unresolved: namely, the standard of likelihood has not been determined, and the legal meaning of "pester" is undefined. Previous judgments have referred to harassment and pestering as interchangeable legal concepts (see *A (HK)* Ltd *and Another v Yeung Yuk Sing and Others,* 2017; *Secretary for Justice v Cheung Kai Yin*, 2016). What Justice Coleman conducted was a preliminary sketch of the balancing test, not an application of the doctrine of proportionality to which he referred (*Secretary for Justice and Commissioner of Police,* 2019, para 44). The nature and form of the exercise of the rights concerned and risks to public order have yet to be delineated (Arai-Takahashi, 2013). We turn now to consider how creation of a public interest defense to doxing might be framed to achieve an acceptable democratic balance.

The Public Interest Defense

In his study of doxing, political philosopher David Douglas (2016) argued that doxing may be justified in cases where the aim is to reveal wrongdoing so as to serve the public interest and the personal data disclosed are confined to that sufficient to reveal the wrongdoing (p. 199). Particular instances of the public interest he had in mind are allegations of legal wrongdoing and establishing a person's identity for the social benefit of making them accountable for offensive behavior (Douglas, 2016, pp. 207–208). At the same time, Douglas (2016) recognized that doxing could turn into the private enforcement of public law and develop into a run-away form of vigilantism (p. 208). In his view, therefore, deanonymizing doxing for the purpose of establishing the identity of a formerly anonymous individual and delegitimizing it for the purpose of contradicting an individual's credibility may both be justified, although the revelation of the specific details of an individual's circumstances that are usually private, obscure, or obfuscated (e.g., his or her home address) is never permissible, as it increases the risk of physical harm to that individual (Douglas, 2016, p. 206).

Further developing Douglas's (2016) argument, I contend that public interest should be introduced as a legal defense for doxing. The disclosure of the personal data of anyone discharging or entrusted with public duty, including politicians, government officials, and police officers, for the purpose of establishing their identity and holding them accountable for alleged legal wrongdoings should be allowed. Other than abuse of power, the category of wrongdoings justifying disclosure of public officials' personal data should include situations where police

officers refuse to show their police identity and warrant card, which is a breach of the Police General Orders.[11] However, the personal data disclosed should be confined to data establishing the identity of the individual concerned and relating directly to the alleged wrongdoing. A good example of such a restriction can be found in the Texas Penal Code, under which there is a rebuttable presumption that a person is interfering with a peace officer if he or she intentionally disseminates the home address, home telephone number, or social security number of the officer concerned or of one of the officer's family members (found in section 38.15(d) (1)). The category of personal data prohibited from disclosure is specific and narrow and, rightly, bears no relation to the officer's discharge of duty or public interest. However, neither this Texas provision nor legislative instruments in Hong Kong clearly articulate a general public interest defense to disclosure of personal data. Singapore perhaps comes closest to articulating such a defense. In 2019, Singapore amended its *Protection from Harassment Act* (*POHA*) to criminalize the act of doxing. Although an accused can defend publication of identifying information about a targeted person on the basis that their conduct was reasonable (*POHA*, 2019, ss. 3, 5, & 6), what reasonable conduct would entail is unclear.

In Hong Kong, it is an offense to disclose any personal data about an individual without their consent if the disclosure causes psychological harm (section 64(2) of the Personal Data Privacy Ordinance [PDPO]). Public interest is a defense only for news workers (section 64(d) PDPO). Proposals have been made to reform the PDPO to tackle doxing, and there have also been suggestions for introducing legislative amendments to specifically address doxing and confer on the Privacy Commissioner statutory powers to request the removal of doxing content from social media platforms or websites, as well as the powers to carry out criminal investigations and prosecutions (Legislative Council Panel on Constitutional Affairs Review of the Personal Data (Privacy) Ordinance, 2020). The focus of the current debate is preoccupied with the need to enlarge the scope of offenses to criminalize the act of doxing. However, it is contended here that a public interest defense should also be considered in any future amendment of the law concerned. While doxing is a form of TFVA, we need to consider who is being exposed, what personal data are being revealed, and why that revelation is taking place. When doxing is carried out for the purpose of exposing the wrongful deeds of those discharging or entrusted with public duty, it is a signal that the public is losing confidence in the ability of established institutions to deliver justice.

Conclusion

Doxing is a complicated and complicating phenomenon and a form of TFVA. However, not all instances of doxing should be treated the same. In contrast with the instances of doxing reported on by Anderson and Wood in this volume, the prevalent trend of doxing against police officers by netizens at this turbulent time in Hong Kong's history reflects a deep yearning for social and legal reform. What might otherwise appear to be a blatant form of user-led data privacy violation and an extreme form of expression may in Hong Kong's case reflect acute awareness, and even anguish, that those entrusted with public duty are abusing their powers unchecked. Doxing for public interest, from this perspective, constitutes an

endeavor to renegotiate what is considered acceptable within a given social and legal context.

Nevertheless, regardless of its cause, doxing remains a contested practice. Whatever the purported purpose, there will always be the lurking question of whether doxing, as an attempt to hold public authorities to account, is the best way to exact social justice. Doxing has serious implications, not least the real risk of physical and psychological harm to targeted individuals. This chapter argues that in political contexts such as the current one in Hong Kong, establishing a public interest defense to doxing would help to strike a better balance between public accountability and privacy. If personal data are a weapon of visibility, what we need is a fair and regulated system of visibility and invisibility.

Postscript

Judges in Hong Kong who were perceived as sympathetic to police and the authorities have become targets of doxing. In November 2020, the HKCFI granted and extended an injunction order restraining unlawful and wilful doxing against judges, any judicial officers, and their family members (Secretary for Justice v Persons Unlawfully and Wilfully Conducting Themselves in Any of the Acts Prohibited under Paragraph 1(a), (b) or (c) of the Indorsement of Claim (2020).

Acknowledgments

The work described in this chapter was fully supported by the General Research Fund (GRF) from the Research Grants Council of the Hong Kong Special Administrative Region (HKU 17623016).

Notes

1. The number of complaints increased markedly, from 57 in 2018 to 4,370 in 2020 (PCPD, 2020a).
2. *Junior Police Officers' Association* (2019, HKCA), reversing the lower court's (*Junior Police Officers' Association*, 2019, HKCFI) decision. Application for judicial review dealing with substantive arguments was heard before the HKCFI on 8 April 2020 (*Junior Police Officers' Association*, 2020), which was partially affirmed by the HKCA (*Junior Police Officers' Association*, 2020).
3. Namely, to decide (1) whether there is a serious issue to be tried in the action (i.e., the claim must not be frivolous or vexatious and must have prospect of success); (2) whether the plaintiff would be adequately compensated by an award of damages for any loss caused by a refusal to grant an interlocutory injunction if they were to succeed at trial; (3) if damages would not be an adequate remedy to the plaintiff, whether, if the injunction were granted, the defendant would be adequately compensated under the plaintiff's undertaking as to damages; and (4) if damages would not be adequate, whether the balance of convenience lies in favor of granting or refusing the interim injunction sought.
4. Relying on the judgment of *Re Leung Chung Hang Sixtus & Another* (2018).
5. In considering the balance of convenience, the Court has to decide whether the cost and inconvenience caused by granting an interlocutory injunction could be

outweighed by the benefits and justice for the applicant. The Hong Kong court must also take into account the interests of the general public in the balancing test (*Turbo Top Ltd v Lee Cheuk Yan*, 2013).

6. Judgment issued on 25 October 2019, amended and reamended on 28 October and 1 November 2019. Further, on 10 December 2019, the Court amended the interim injunction order such that Special Constables would also be protected (Hong Kong Police Force, 2019).
7. The reference to "interfere" was removed by Justice Coleman in a subsequent application for the continuation of the interim injunction as the word was "insufficiently precise" (*Secretary for Justice and Commissioner of Police*, 2019b, para 48).
8. The association applied as a party who may be affected by the injunction order but not as a named defendant nor other party to the action (*Secretary for Justice and Commissioner of Police*, 2019b, paras 9–10). News activity is defined under section 61(3) of the Personal Data (Privacy) Ordinance (Cap. 486).
9. Article 84 of the Basic Law.
10. Freedom of expression is guaranteed by article 16 of the HKBOR while right to privacy by article 14 of the same document.
11. The relevant provision of the Hong Kong Police General Orders is not available to the public. Reference to this requirement can be found at the Independent Police Complaints Council (2012) Special Report (para 2.13.11).

References

A (HK) Ltd and Another v Yeung Yuk Sing and Others. (2017). HKCFI 1926.

American Cyanamid Co. (No. 1) v Ethicon Ltd. (1975). UKHL 1.

Amnesty International. (2019a, June 21). Evidence of Hong Kong police violence verified. *Amnesty International [News release]*. Retrieved from https://www.amnesty.org/en/latest/news/2019/06/hong-kong-police-violence-verified/

Amnesty International. (2019b, September 19). New evidence of shocking police abuses against Hong Kong protesters. *Amnesty International [News release]*. Retrieved from https://www.amnesty.org/en/latest/news/2019/09/hong-kong-arbitrary-arrests-brutal-beatings-and-torture-in-police-detention-revealed/

Arai-Takahashi, Y. (2013). Proportionality (chapter 19). In *Oxford handbook of international human rights law*. Retrieved from https://www.oxfordhandbooks.com/view/10.1093/law/9780199640133.001.0001/law-9780199640133-e-20

BBC News (2019, October 14). Hong Kong protests explained in 100 and 500 words. BBC News. Retrieved from https://www.bbc.com/news/world-asia-china-49317695

Cameron v Liverpool Victoria Insurance. (2019). UKSC 6.

Chan, E., & Blundy, R. (2019, November 1). "Bulletproof" China-backed doxxing site attacks Hong Kong's democracy activists. *Hong Kong Free Press*. Retrieved from https://www.hongkongfp.com/2019/11/01/bulletproof-china-backed-doxxing-site-attacks-hong-kongs-democracy-activists/

CNN. (2020). Hong Kong protests. Retrieved from https://edition.cnn.com/specials/asia/hong-kong-protests-intl-hnk

Cooper, S. (2019, March 28). What is doxxing (with examples) and how do you avoid it. *Comparitech*. Retrieved from https://www.comparitech.com/blog/vpn-privacy/what-is-doxxing-how-to-avoid/

Douglas, D. M. (2016). Doxing: A conceptual analysis. *Ethics and Information Technology*, *18*(3), 199–210. doi:10.1007/s10676-016-9406-0

Fugitive Offenders and Mutual Legal Assistance in Criminal Matters Legislation (Amendment) Bill. (2019). Retrieved from https://www.legco.gov.hk/yr18-19/english/bills/brief/b201903291_brf.pdf

Graham-Harrison, E., Kuo, L., & Yu, V. (2019, October 6). A battle for the soul of the city: Why violence has spiralled in the Hong Kong protests. *The Guardian*. Retrieved from https://www.theguardian.com/world/2019/oct/06/a-battle-for-the-soul-of-the-city-why-violence-has-spiralled-in-the-hong-kong-protests

Hale, E. (2019, September 20). Hong Kong protests: Tech war opens up with doxxing of protesters and police. *The Guardian*. Retrieved from https://www.theguardian.com/world/2019/sep/20/hong-kong-protests-tech-war-opens-up-with-doxxing-of-protesters-and-police

HKSAR v Chan King Kei. (2020). [2020] HKDC 1020 (in Chinese).

Hong Kong Police Force, HKSAR. (2019, December 11). Interim injunction order of the high court (HCA 1957/2019) – doxxing and harassment against police officers, special constables and their families. *Hong Kong Police Force [News release]*. Retrieved from https://www.police.gov.hk/ppp_en/03_police_message/iio_1957.html

Independent Police Complaints Council, HKSAR. (2012). Final report on complaint cases arising from the visit by the Vice Premier Mr Li Keqiang. Retrieved from https://www.ipcc.gov.hk/doc/en/report/Other/Report_f_en.pdf

Junior Police Officers' Association of the Hong Kong Police Force v Electoral Affairs Commission and others. (2019a). [2019] HKCA 1197.

Junior Police Officers' Association of the Hong Kong Police Force v Electoral Affairs Commission and others. (2019b). [2019] HKCFI 2628.

Junior Police Officers' Association of the Hong Kong Police Force v Electoral Affairs Commission and others. (2020a). [2020] HKCA 352.

Junior Police Officers' Association of the Hong Kong Police Force v Electoral Affairs Commission and others. (2020b). [2020] HKCFI 554.

Kilpatrick, R. H. (2019, August 16). "An eye for an eye": Hong Kong protests get figurehead in woman injured by police. *The Guardian*. Retrieved from https://www.theguardian.com/world/2019/aug/16/an-eye-for-an-eye-hong-kong-protests-get-figurehead-in-woman-injured-by-police

Lau, C., & Ng, K. (2019, September 20). Hong Kong newspaper gets injunction against reporters' doxxing. *South China Morning Post*. Retrieved from https://www.scmp.com/news/hong-kong/law-and-crime/article/3029573/hong-kong-newspaper-apply-daily-gets-injunction

Lee, D. (2013, April 19). Boston: Internet detectives get it wrong. *BBC News*. Retrieved from https://www.bbc.com/news/technology-22214511

Lee, F. L. F. (2019, October 16). Our research in Hong Kong reveals what people really think of the protesters – and the police. *The Independent*. Retrieved from https://www.independent.co.uk/voices/hong-kong-protests-police-violence-public-opinion-polling-support-a9158061.html

Legislative Council Panel on Constitutional Affairs Review of the Personal Data (Privacy) Ordinance. (2020, 20 January). LC Paper No. CB (2)512/19–20(03).

Leung, C. (2020, January 22). Police officers 'warned' for mishandling reporters' personal data. *South China Morning Post*. Retrieved from https://www.scmp.com/news/hong-kong/law-and-crime/article/3047073/police-officers-received-verbal-warnings-holding

Lo, C., & Mok, D. (2020, January 29). Hong Kong protests: Radicals in bomb threat against police living quarters. *South China Morning Post*. Retrieved from https://

www.scmp.com/news/hong-kong/law-and-crime/article/3048133/hong-kong-protests-petrol-bombs-thrown-kwai-chung

Lustbader, S., & Gullapalli, V. (2019, January 15). The ethics of doxing and the politics of public shaming. *The Appeal*. Retrieved from https://theappeal.org/the-ethics-of-doxing-and-the-politics-of-public-shaming/

MacAllister, J. M. (2017). The doxing dilemma: Seeking a remedy for the malicious publication of personal information. *Fordham Law Review*, *85*(5), 2451–2483.

NYU Tandon School of Engineering. (2017, November 7). First large-scale doxing study reveals motivations and targets for cyber bullying. *ScienceDaily*. Retrieved from https://www.sciencedaily.com/releases/2017/11/171107122918.htm

Privacy Commissioner for Personal Data, Hong Kong [PCPD]. (2020a, January 12). Privacy commissioner responds to public concern about disclosure of a reporter's personal data [Media Statement]. Retrieved from https://www.pcpd.org.hk//english/news_events/media_statements/press_20200108.html

Privacy Commissioner for Personal Data, Hong Kong [PCPD]. (2020b, November 3). First doxxing case sentenced for contravention of PDPO privacy commissioner urges the public not to flout the law [Media Statement]. Retrieved from https://www.pcpd.org.hk/english/media/media_statements/press_20201103.html

Protection from Harassment (Amendment) Act, 17 October 2019, with effect on 1 January 2020.

Re Leung Chung Hang Sixtus & Another. (2018). HKCFI 1869.

Secretary for Justice and Commissioner of Police v Persons Unlawfully and Wilfully Conducting Themselves in any of the Acts Prohibited under Paragraph 1(a), (b) or (c) of the Indorsement of Claim. (2019a). [2019] HCA1957/2019.

Secretary for Justice and Commissioner of Police v Persons Unlawfully and Wilfully Conducting Themselves in any of the Acts Prohibited under Paragraph 1(a), (b) or (c) of the Indorsement of Claim. (2019b). [2019] HKCFI 2773.

Secretary for Justice v Persons Unlawfully and Wilfully Conducting Themselves in Any of the Acts Prohibited under Paragraph 1(a), (b) or (c) of the Indorsement of Claim. (2020). [2020] HKCFI 2785.

Secretary for Justice v Cheung Kai Yin. (2016). HKCA 457.

Snyder, P., Doerfler, P., Kanich, C., & McCoy, D. (2017). Fifteen minutes of unwanted fame: Detecting and characterizing doxing. In *Proceedings of the 2017 Internet Measurement Conference*, London (pp. 432–444). doi:10.1145/3131365.3131385

Tenold, V. (2018, July 26). To doxx a racist. *The New Republic*. Retrieved from https://newrepublic.com/article/150159/doxx-racist

The Economist. (2017, May 6). The world's most valuable resource is no longer oil, but data Retrieved from https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

Trottier, D. (2017). Digital vigilantism as weaponisation of visibility. *Philosophy & Technology*, *30*(1), 55–72. doi:10.1007/s13347-016-0216-4

Trottier, D. (2019). Denunciation and doxing: Towards a conceptual model of digital vigilantism. *Global Crime*, *21*, 1–17. doi:10.1080/17440572.2019.1591952

Turbo Top Ltd v Lee Cheuk Yan. (2013). HKCFI 723.

Woolf, N. (2015, November 6). Anonymous leaks identities of 350 alleged Ku Klux Klan members. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2015/nov/06/anonymous-ku-klux-klan-name-leak