

PERSONAL DATA PROTECTION COMMISSION

[2018] SGPDPC [3]

Case No DP-1612-B0423

In the matter of an investigation under section 50(1) of the Personal Data
Protection Act 2012

And

My Digital Lock Pte. Ltd.

... Organisation

DECISION

My Digital Lock Pte. Ltd.

[2018] SGPDPC [3]

Yeong Zee Kin, Deputy Commissioner — Case No DP-1612-B0423

12 February 2018

1 This is the third complaint lodged by the Complainant against My Digital Lock Pte. Ltd. (“the **Organisation**”). The first complaint was the subject of the decision in *Re My Digital Lock Pte. Ltd.* [2016] SGPDPC 20. Investigations were discontinued in respect of the second complaint, as the facts and allegations relied upon in the complaint were closely linked to legal proceedings which were ongoing at the time between the Complainant and the Organisation, and it was determined that the matter was best dealt with through the ongoing legal proceedings. In this third complaint, after a review of the material facts, I exercised my discretion under section 50 of the Personal Data Protection Act 2012 (“**PDPA**”) to discontinue investigations. I set out hereunder the reasons for the exercise of my discretion in this case.

Background

2 Sometime in October 2015, the Complainant purchased a digital lock from the Organisation for his home. Shortly after, the Complainant and the sole director of the Organisation (“**Sole Director**”) became involved in a dispute concerning alleged defects in the Organisation’s product. The Organisation then took out civil action in defamation in relation to certain remarks that were allegedly made by the Complainant concerning the Organisation’s business.

3 Subsequently, the Sole Director posted screenshots of WhatsApp messages, as well as photographs, on his personal Facebook page (“**Facebook Page**”). These WhatsApp messages and photographs were related to the then ongoing dispute between the Organisation and the Complainant. The personal data in the WhatsApp messages comprised the Complainant’s contact details, namely, his mobile phone number and residential address.

4 On 4 January 2016, the Complainant lodged a complaint with the Personal Data Protection Commission (“**Commission**”) after discovering the unauthorised disclosure of his personal data on the Facebook Page. In respect of this complaint, a warning was issued to the Organisation for breaching its obligations under sections 13 and 24 on 4 November 2016. See *Re My Digital Lock Pte. Ltd.* [2016] SGPDPDPC 20 for the detailed grounds of this decision.

5 On 9 September 2016, before the decision for the first complaint was issued, the Complainant lodged a second complaint concerning the Organisation’s disclosure of his personal data on a publicly accessible blog. This blog was the personal blog (“**Blog**”) of the Sole Director who had set it up with the intent to respond to the various allegations made by the Complainant about the Organisation’s business. The Sole Director posted images and screenshots of the online allegations that had been made by the Complainant on various websites and forums, and appended his personal response to each of these allegations.

6 One of the images the Sole Director posted on his Blog was a letter sent by the Organisation’s solicitors to the Complainant in April 2016. The screenshot was of an open window, in which was displayed a letter and the file name of this document was displayed in the title bar of the open window (“the **Letter**”). The Complainant’s name formed part of the file name of the Letter.

Although the file name displayed in the window title was not redacted, the Sole Director had taken care to redact the name and residential address of the Complainant in the body of the Letter that was displayed in the open window. Investigations into the matter were discontinued as the matters arising from the complaint would have been more appropriately dealt with as part of the then ongoing legal proceedings between the parties. Any claims or allegations made, or any facts relied upon, by either party would have very likely been relevant to the civil proceedings as the Blog was set up by the Sole Director to refute the alleged defamatory remarks made by the Complainant – this goes to the crux of the civil dispute between the parties.

7 I would, at this juncture, highlight the decision in *Re M Star Movers & Logistics Specialist Pte Ltd* [2017] SGPDPC 15 (“*M Star Movers*”) and reiterate that an organisation cannot be prevented from making reasonable and proportionate responses to defend itself from allegations made against it, even if personal data is disclosed in doing so. In *M Star Movers*, action was taken against the organisation because the personal data that was disclosed was disproportionate in the circumstances and therefore the organisation was found to have acted unreasonably. In the second complaint, the Complainant had chosen to air his grievances with the Organisation on multiple public websites and forums. As investigations were discontinued, the Commissioner did not have to address the issue whether naming the Complainant in his Blog in an attempt to refute the allegations made would have been a reasonable and proportionate response in the circumstances.

8 The Complainant made his third complaint (“**Complaint**”) on 5 November 2016. This time, the Complainant referred the Commission to a Facebook post where the Organisation had posted a copy of a police report that the Organisation’s staff had made about a person who was allegedly harassing

the staff of the Organisation. The Complainant was named by the Organisation's member of staff as the one who was carrying out such harassing acts.

9 Investigations commenced on 8 December 2016. I subsequently directed that investigations into the case be discontinued and an advisory notice issued to the Organisation. Although my decision was a discontinuance under section 50(3) of the PDPA, I thought it helpful to provide detailed reasons for doing so. This decision touches on issues that are fundamental to the administration and enforcement of the PDPA, namely:

- (a) when does a document containing personal data that is the subject matter of a complaint become one that the Commissioner (or his delegates) will consider exercising enforcement jurisdiction over;
- (b) how does the PDPA sit within the framework of statutory and common law rights that collectively provide safeguards to the privacy of individuals in Singapore; and
- (c) how does the Commissioner discern between a breach of the PDPA that ought to be investigated and cases for which private action in the civil courts enforcing the abovementioned framework of laws provide better remedies to safeguard the privacy of individuals?

Documents containing personal data

10 We start with the definition of "personal data" in section 2 of the PDPA. This is a broad definition:

"personal data" means data, whether true or not, about an individual who can be identified —

- (a) from that data; or

(b) from that data and other information to which the organisation has or is likely to have access.

11 There are certain types of information that in and of themselves are capable of identifying an individual. The Advisory Guidelines on Key Concepts in the PDPA (revised on 27 July 2017) (“**Key Concepts Guidelines**”) at [5.10] provides a list of information that is considered to be capable of doing so. While such information is capable of identifying an individual, it does not necessarily mean that anyone in possession of the information will be able to do so. The touchstone used to compile the list is the one-to-one relationship of the information and the individual. Information on the list is not typically associated with more than one individual, either scientifically (eg biometric signature and DNA profile), by convention (eg NRIC number) or as a matter of social norms (eg personal mobile phone number).

12 At a higher level of abstraction, we consider the question when does a document contain information about an individual? What are the factors that the Commissioner considers in deciding whether the use or disclosure of personal data in documents draws its scrutiny through the lens of the PDPA? The remarks that follow apply not only to textual documents but images (eg photographs that capture the image of an identifiable individual in the Advisory Guidelines on the PDPA for Selected Topics (revised on 28 March 2017) at [4.2]) and audio visual documents (eg CCTV footage in *Re Management Corporation Strata Title Plan No 2956* [2017] PDP Digest 238).

13 In the UK case of *Durant v. Financial Services Authority* [2003] EWCA Civ 1746 (“*Durant*”), the Court of Appeal adopted the “biographically significant information” test where the recording of the information goes beyond the mere “*putative data subject’s involvement in a matter or an event that has no personal connotations, a life event in respect of which his privacy*

could not be said to be compromised". The focus of the information should be the data subject rather than some other person, or some transaction or event in which the data subject may have figured or have had an interest in: *Durant* at [28].

14 In a subsequent case of *Edem v. IC & Financial Services Authority* [2014] EWCA Civ 92 ("*Edem*"), the English Court of Appeal cast doubt on the biographically significant information test as the sole criterion. Without expressly overruling the earlier decision in *Durant*, the court held that the disclosure of the names of three individuals could be withheld on the basis that they constituted personal data upon which the UK Data Protection Act 1998 was applicable. The court, agreeing with the Information Commissioner's Office ("*ICO*") Data Protection Technical Guidance, took the view that it was not "*always necessary to consider 'biographical significance' to determine whether data is personal data*" – the only time to consider the "biographical significance" of the data is where the information is not "*obviously about*" an individual or clearly "*linked to*" him: *Edem* at [21].

15 In assessing whether an unauthorised disclosure or access of information about an individual in a document ought to be one that requires scrutiny under the PDPA, the approach that ought to be taken is to first consider whether the document is clearly about an individual or individuals. Hence, flight manifests that serve the function of conveying information about the individuals on the flight will qualify: see *Re Tiger Airways Singapore Pte Ltd and others* [2017] SGPDPC 6. Similarly, a letter that is intended to identify a former employee to the organisation's customers will also qualify: see *Re Jump Rope (Singapore)* [2016] SGPDPC 21. As the collection of documents increases, the purpose of recording or conveying information about individuals becomes indisputable. Hence, mishandling of customers' insurance records (eg *Re Ang Rui Song*

[2017] SGPDPC 13), and breaches of information systems containing customer or membership records (eg *Re Orchard Turn Developments Pte. Ltd.* [2017] SGPDPC 12) are cases where the documents were clearly about individuals.

16 Even if a document is not clearly about the individual, such as the documents in *Durant* which pertained to Mr Durant’s complaint to the Financial Services Authority (“FSA”) about the conduct of Barclays Bank or about the FSA’s own conduct in their investigations of his complaint, the Commissioner would consider whether the information is biographically significant. Consider instant messaging communications, which will contain the identifier associated with the author of each message: see *Re Executive Coach International Pte. Ltd.* [2017] SGPDPC 3. These identifiers are automatically inserted into the communication as a function of the communication system. Similarly, an exchange of social media posts will contain identifiers of who wrote each post, as will emails contain the sender and intended recipients’ names and email addresses. In and of themselves, such identifiers are intended to identify the originator (or recipient) but does it mean that the *purpose of each such message* is to convey information about the originator by reason only of the inclusion of the identifier? I do not think so. It is necessary to consider the content of the message. The content of the message must convey information about one or more individuals. Thus in *Re Black Peony* [2017] PDP Digest 218, it was decided that private communications such as WhatsApp messages *per se* will not invariably be considered personal data.

17 This approach applies to all types of documents, textual as well as multimedia. This may be relevant in cases in which the Commissioner exercises his discretion to suspend, discontinue or refuse to conduct an investigation.

18 At this juncture, I take the opportunity to highlight that an individual has two avenues through which he may address his concerns of a potential breach of the PDPA by an organisation. The individual may submit a complaint to the Commission. Where the individual has suffered loss or damage directly as a result of the contravention, the individual may commence civil proceedings against the organisation under section 32 of the PDPA.

19 Where the individual chooses to lodge a complaint with the Commission, the Commissioner (and his delegates) has discretion under section 50(3) of the PDPA to suspend, discontinue or refuse to conduct an investigation. One of the circumstances in which the Commissioner may exercise his discretion under section 50(3) of the PDPA is where the Commissioner deems that the severity of the potential breach does not warrant taking any further action. Data protection regulators in other jurisdictions, such as the UK Information Commissioner's Office¹, similarly take the same approach, as clearly every single data protection complaint cannot be investigated. In determining the severity of the potential breach, the Commissioner may consider, amongst other things, the nature of the personal data affected, the number of people affected, whether the breach is due to systemic issues and the likely effect on the individuals concerned. The biographical significance test would be relevant when considering the nature of the personal data affected and the likely effect on the data subject.

20 In the present case, the document concerned was a police report made by a member of the Organisation's staff concerning harassing conduct purportedly carried out by the Complainant. The disclosure of the

¹ United Kingdom Information Commissioner's Office. *How we deal with complaints and concerns – A guide for data controllers* at pg. 4

Complainant's identity was therefore one of the purposes of the report and since the allegation in the report was about the Complainant's purportedly harassing conduct, the content of the report was therefore potentially of biographical significance. I have nevertheless decided to exercise my discretion in this case to discontinue investigations in this matter. The following discussion will explain my exercise of discretion. A caveat ought to be inserted at this juncture that this is not intended to be a comprehensive compendium of all considerations in the exercise of discretion. There will be future cases where different aspects of the discretion will be explained, within the factual matrix of those cases.

The intersection between the law protecting privacy and personal data protection

21 In order to explain the exercise of my discretion to discontinue investigations, it is necessary to understand the interaction between the applicable common law principles – by which I mean also to include statutory torts – that protect privacy and the operations of the PDPA. Even if the information in a document has a purpose of conveying information about an individual, it is not necessarily the case that the most appropriate remedies are in the civil administrative enforcement provisions of the PDPA. While it has oft been said that there is no right to privacy under common law, this statement ought to be re-examined in light of developments in both the common law and statutory torts in recent past. Without going into a lengthy dissertation, I posit that while it is probably still true that the common law does not recognise a *general right* to privacy, there exists today a framework of common law and statutory torts that collectively protect an individual's privacy. Individuals are therefore able to prosecute their claims for invasions into their privacy by

private action before the civil courts much more effectively today than in the past.

22 The Singapore courts have not made any explicit pronouncements that a *general tort of privacy* exists nor that there is explicit provision for the protection of privacy as a fundamental right in our Constitution; neither is there an omnibus privacy legislation in our statute books: see Gary Chan Kok Yew & Lee Pey Woan, *The Law of Torts Singapore* (2nd Ed, 2015) at [16.011]. The starting point in Singapore is therefore not very different from the common law. *Kaye v. Robertson* [1991] FSR 62 (“*Kaye v. Robertson*”) has often been cited as authority for the proposition that there is no right to privacy in the common law. *Kaye v. Robertson* was a case which involved journalists intruding into the hospital room of a well-known actor and taking photographs of him. The UK Court of Appeal acknowledged that “[it] is well-known that in English law there is no right to privacy, and accordingly there is no right of action for breach of a person’s privacy”: per Glidewell LJ. at 66. This position was confirmed in *Wainwright v. Home Office* [2004] 2 AC 406 when the House of Lords declined to recognise a general right of privacy which would extend to physical privacy interferences. Although our Court of Appeal traversed the authorities in the case of *ANB v. ANC* [2015] 5 SLR 522 (“*ANB v. ANC*”), the question whether a common law right of privacy should be recognised was intentionally left open: see *ANB v. ANC* at [20] – [23].

23 Privacy, as a standalone common law right, is steadily gaining recognition in some parts of the Commonwealth. Recent developments in Canada and New Zealand that recognise a general common law right to seclusion are discussed in a subsequent section: see discussion below at [24]. Most recently, the Indian Supreme Court in the case of *Justice K.S. Puttaswamy (Retd.) and ANR v. Union of India and Ors Writ Petition (Civil) No 494 of 2012*

(“*Puttaswamy*”) recognised the right to privacy as a constitutional right. Although the decision did not address the question whether privacy rights were enforceable as a common law tort, it was clear that the majority of the Supreme Court felt that the right to privacy was a fundamental right protected by the Indian Constitution.

24 It is unlikely that our courts would take the same approach as in *Puttaswamy*. In *Lim Meng Suang v. Attorney-General* [2015] 1 SLR 26, the Singapore Court of Appeal held that the right to privacy and personal autonomy should not be read into the phrase “life or personal liberty” in Article 9 of the Singapore Constitution: at [44] – [47]. The Court of Appeal made it clear that there is unlikely to be a constitutional right to privacy; the appellants cannot “*obtain by the (constitutional) backdoor what they cannot obtain by the (private law) front door*”: at [49]. However, the Court of Appeal left it open for there to be a right to privacy “*developed by way of the private law on privacy instead*”: at [49].

25 While our courts have not recognised the existence of a general right to privacy that is an actionable tort, or a fundamental right protected by our Constitution, that is not to say that our laws do not protect different aspects of privacy. An appreciation of how privacy is protected by a framework of common law and statutory torts is a necessary primer for understanding the interaction between the common law principles that protect privacy and the operation of the PDPA. It is apposite to preface the discussion by drawing a distinction between those torts that indirectly protect privacy interests (eg trespass to the person or land and nuisance), and the bundle of rights that a general right to privacy protects. It is the latter that we train our focus on.

26 What is privacy? A useful definition with which to commence our discussion is that which was provided by Samuel D. Warren and Louis D. Brandeis – the right to be let alone: see “The Right to Privacy” (1890) Harvard L. Rev. Vol. 4(5) 193 at 195. A helpful framework for discerning the contours of this right was offered by William L. Prosser (see “Privacy” (1960) 48 Cal. L. Rev. 383 at 389 (“**Prosser, Privacy**”)):

- (a) the right to seclusion – the right to prevent intrusions into one’s seclusion that exists independently of the tort of trespass to person or property;
- (b) the right to prevent publication of private communication – recent common law developments have started to recognise the existence of this right independently of the law of confidentiality;
- (c) the right to prevent the appropriation of identity; and
- (d) the right to prevent false publicity.

27 The Prosser categorisation provides a useful framework for examining the different aspects of privacy. It is necessary to understand how this bundle of rights are currently protected by common law and statutory torts in order to appreciate the dynamics between remedies under these laws protecting an individual’s privacy and the Commissioner’s role in the enforcement of the PDPA, which protects informational privacy and therefore sits within the penumbra of the laws protecting privacy.

Right to seclusion

28 Intrusion upon seclusion or solitude involves an invasion of a victim’s private space or affairs. Some torts that are premised on trespass to property or

person protect aspects of the right to seclusion, but to be effective, this right ought not be dependent on an invasion of one's person or property. The tort of privacy based on the right to seclusion has been recognised in other countries. In New Zealand, the High Court recognised the common law tort of intrusion upon seclusion as a standalone tort in *C v. Holland* [2013] 3 LRC 78 ("*C v. Holland*"). In that case, the claimant was a young woman who suffered deep distress when she discovered that her boyfriend's flatmate had covertly installed a camera in the roof cavity above the bathroom to film her undressing and showering. To establish a claim under the tort of intrusion upon seclusion, a claimant had to show (see *C v. Holland* at [94]):

- (a) an intentional and unauthorised intrusion;
- (b) into seclusion (namely, intimate personal activity, space or affairs);
- (c) involving infringement of a reasonable expectation of privacy; and
- (d) that is highly offensive to a reasonable person.

29 In Canada, the courts have also recognised a common law right of action for intrusion upon seclusion in the case of *Jones v. Tsige* (2012) ONCA 32 ("*Jones v. Tsige*"). In that case, the defendant, who was in a relationship with the claimant's former husband, and who worked for the same bank as the claimant but in a different branch, used her workplace computer to gain access to the claimant's private banking records 174 times, for the alleged purpose of confirming whether the claimant's former husband was paying child support. In confirming the existence of the intrusion-based privacy tort, the Ontario Court of Appeal adopted as essential elements the formulation in the US Restatement

of the Law, Second, Torts (1977) §652: “[o]ne who intentionally intrudes, physically or otherwise, upon the seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the invasion would be highly offensive to a reasonable person”: *Jones v. Tsige* at [70].

30 In Singapore, the High Court, in the case of *Malcomson Nicholas Hugh Bertram v. Naresh Kumar Mehta* [2001] 3 SLR(R) 379 (“**Malcomson**”), was perhaps a little ahead of the times when it took a decidedly different turn from the general common law position by recognising a tort of intentional harassment. The elements of this tort were (a) knowingly engaging in (b) a sufficiently repetitive course of conduct that would (c) cause worry, emotional distress or annoyance to another person: *Malcomson* at [31]. The Court of Appeal in *Tee Yok Kiat v. Pang Min Seng* [2013] SGCA 9 did not question the existence of the tort of intentional harassment. The similarities and differences between this tort of intentional harassment and the more recent torts of intrusion upon seclusion would have provided ample fodder for commentary. Unfortunately, while the New Zealand and Canadian courts were establishing equivalent torts of privacy, the High Court in the subsequent case of *AXA Insurance Singapore Pte Ltd v. Chandran s/o Natesan* [2013] 4 SLR 545 at [8] – [10], cast doubt on the existence of this common law right and called for legislative intervention if such a right ought to be recognised.

31 The tort of harassment is now enshrined in sections 3 and 4 of the Protection from Harassment Act (Cap. 256A) (“**POHA**”). POHA had expressly abolished the common law tort of intentional harassment and established that no civil proceedings shall be brought for the tort of harassment except as a statutory tort under section 14 of POHA. POHA also introduced a statutory tort

of unlawful stalking: section 7. The operation of these sections are briefly described in *Ting Choon Meng v. Attorney-General* [2016] 1 SLR 1248 at [15]:

- (a) Section 3 makes it an offence for a person to behave or communicate in a “threatening, abusive or insulting” way with the intention of causing, and actually causing, “harassment, alarm or distress” to a victim;
- (b) Section 4 makes it an offence to behave or communicate in a “threatening, abusive or insulting” way towards a victim who is likely to be caused “harassment, alarm or distress”; and
- (c) Section 7 makes “unlawful stalking” an offence, and defines this as engaging in a course of conduct which involves acts or omissions associated with stalking and which causes “harassment, alarm or distress” to a victim, provided that there was an intention to cause such “harassment, alarm or distress” or at least knowledge that this was a likely outcome.

32 Collectively, these statutory provisions can now be relied upon to protect one’s seclusion from intrusion. These are still relatively new statutory torts and time will tell if they provide the same umbrella of protection as a general tort of intrusion upon seclusion. If the excesses of the paparazzi caused alarm or distress to Mr Kaye in *Kaye v. Robertson*, he may now resort to the statutory tort of harassment for relief. Similarly, the victim in *C v. Holland* may now seek relief against her boyfriend’s flatmate under the tort of unlawful stalking. The protection offered by these statutory torts no doubt covers physical intrusions, but may extend to online activities where the *communication content* amounts to harassment or stalking conduct. In *Benber Dayao Yu v. Jacter Singh* [2017] 5 SLR 316 at [25], it was held that “*harassing conduct on the Internet, such as those in the Web post in the present case would be covered by ss 3 and 4 of the POHA.*”

33 However, the victim in *Jones v. Tsige* probably may not be able to resort to these statutory torts to safeguard her bank accounts from the prying eyes of the defendant. But there is room for the PDPA, which deals with *informational*

privacy, to operate in conjunction with the aforementioned statutory torts to protect intrusions into seclusion. The factual matrix of *Jones v. Tsighe* can potentially be a breach of the protection obligation on the part of the bank (but may provide no reliefs against the former husband or his lover, the defendant, as they were acting in a domestic or personal capacity). Likewise, the factual matrix of *Kaye v. Robertson* can give rise to a claim for collection of personal data without consent. Both of these breaches can now be enforced as private actions under section 32 of the PDPA. The right of private action under the PDPA protects *informational* privacy which is complementary to but distinct from the protection of one's seclusion, although these rights may overlap and co-exist.

34 It is open to debate whether there is still room for a common law tort of intrusion upon seclusion, although the contours of such a tort will be heavily influenced by the statutory torts under POHA and PDPA. This is not the place nor is it my intention to discuss the similarities and differences between the range of conduct prohibited by the statutory torts under POHA and PDPA, and those categories prohibited by a common law tort that prevents intrusion upon seclusion. Before leaving this category, it suffices for me to make the following observations. *First*, the state of our laws does not leave one's right to seclusion unprotected; as can be seen from the foregoing discussion, there are statutory torts that collectively offer a significant degree of protection of one's seclusion from unwanted intrusion. These are early days and the jurisprudence can be expected to grow as more cases are brought before the courts, and more commentaries are published. *Second*, a plaintiff seeking relief against his intruder by filing a civil claim can pursue one or more of the statutory torts in POHA and PDPA, whereas a complaint lodged with the Commission is limited to redress for PDPA breaches. *Third*, our courts may well take a leaf from the common law developments in Canada and New Zealand and find sufficient

room for the development of a *general* tort of intrusion into seclusion that complements the statutory torts under POHA and PDPA. This development of the common law may only be declared by the courts, and then only when the appropriate case goes before them. Therefore, if the true mischief is an intrusion upon one's seclusion, a civil claim before the courts is more likely to yield an effective set of reliefs than a complaint to the Commission.

Right to prevent publication of private communication

35 Another strand of development in the right of privacy is the recognition of the right to prevent publication of private communication. This has now been recognised as a new cause of action distinct from an action for breach of confidence in two House of Lords cases: see *Campbell v. MGN Ltd* [2004] 2 AC 457 ("**Campbell**") and *Douglas v. Hello! Ltd* [2008] 1 AC 1 ("**Douglas**"). In *Campbell*, the House of Lords held that where the invasion of privacy is occasioned by a wrongful disclosure of personal information, "*the essence of the tort is better encapsulated now as misuse of private information*": per Lord Nicholls of Birkenhead at [14]. In *Douglas*, it was explicitly recognised that "traditional" breach of confidence and misuse of private information had become separate and distinct wrongs: per Lord Nicholls of Birkenhead at [255]. The key development in this tort is, to my mind, the availability of remedies even where the private communication does not have the necessary quality of confidence, which had hitherto been the death knell to any action based on the breach of confidentiality: see *Coco v. AN Clark (Engineers) Ltd* [1968] FSR 415. While confidentiality protects secrecy, the cause of action for misuse

involves the identification of private information as “*something worth protecting as an aspect of human autonomy and dignity*”: *Campbell* at [50].²

36 While this development in the UK may be viewed as being necessitated by their obligation to give effect to the EU Human Rights Convention as enacted in the UK Human Rights Act 1998, the Singapore Court of Appeal in *ANB v. ANC* observed that the English common law had recognised a right to privacy as long ago as the 1990 decision of *Attorney-General v. Observer Ltd* [1990] 1 AC 109. The relationship between the right of privacy and breach of confidence was also articulated in *Hellewell v. Chief Constable of Derbyshire* [1995] 4 All ER 473 at 476:

“If someone with a telephoto lens were to take from a distance and with no authority a picture of another engaged in some private act, his subsequent disclosure of the photograph would, in my judgment as surely amount to a breach of confidence as if he had found or stolen a diary in which the act was recounted and proceeded to publish it. In such a case, the law would protect what might reasonably be called a right of privacy, although the name accorded to the cause of action would be breach of confidence”.

37 The Court of Appeal in *ANB v. ANC* recognised that such a right had emerged in the UK from the law of breach of confidence. Developments in other common law jurisdictions – New Zealand was specifically mentioned – and the statutory developments in Singapore – principally, the enactment of the POHA and PDPA – were referred to as signalling an increasing recognition of the need

² As Lord Hoffman said in *Campbell v. MGN Limited* [2004] 2 AC 457: “*the new approach takes a different view of the underlying value which the law protects. Instead of the cause of action being based on the duty of good faith applicable to confidential personal information and trade secrets alike, it focuses upon the protection of human autonomy and dignity – the right to control the dissemination of information about one’s private life and the right to the esteem and respect of other people*” (at [51]). See also, Tugendhat and Christie, *The Law of Privacy and the Media*, 2nd ed. by Mark Warby QC, Nicole Moreham & Iain Christie eds., (Oxford: OUP, 2011) at [5.04].

to protect personal privacy: see *ANB v. ANC* at [22]. Whilst the Court of Appeal stopped short of making an express determination on the issue as it was deciding an interlocutory appeal, it recognised that the question of “*whether we should afford, like the courts in England and various other jurisdictions, protection to one’s privacy by way of the law of confidence regardless of whether such a right is guaranteed under the Constitution ... [the] extent to which we should adopt such jurisprudence, ie, the circumstances under which the law of confidence would extend its protection to private information acquired without consent*” gave rise to serious questions to be tried. The Court of Appeal concluded by cautioning that it was “*by no means endorsing or encouraging, the identification of a right to protection of private information under our law of confidence*”: *ANB v. ANC* at [23].

38 This right to prevent misuse of private communication and informational privacy often – but not necessarily always – coexist. Private communications that interlocutors are keen to prevent misuse of often contain information that is personal or intimate, and frequently personal information of a biographical nature. A couple of observations may be made. *First*, the right to prevent the misuse of *private information* seeks to prohibit the publication of information that was meant to be private. The PDPA prevents, in this context, disclosure of *personal data* without authority. The range of communications that the common law right protects is broader, as it extends beyond personal information to communications content. For example, an intimate conversation within the confines of a taxicab may not contain any personal information. The right to prevent its publication lies with the common law right to prevent publication of private information, not with the PDPA. Also, a document that contains personal information incidentally (eg names and contact details in a letter or email) may not be one that the Commissioner will consider exercising enforcement jurisdiction over: see discussion above, at [15] *et seq*, on whether

the document conveys personal information or the information is biographically significant.

39 *Second*, the common law right will protect private information *in the nature of personal data* from publication even if the information is publicly available. Thus, the taking of a photograph in a public space may be an infringement of privacy, if it intrudes into the individual’s personal space: per Lord Hoffman in *Campbell at* [75], “*the widespread publication of a photograph of someone which reveals him to be in a situation of humiliation or severe embarrassment, even if taken in a public place, may be an infringement of the privacy of his personal information*”. The taking of a photograph in a public place would attract the “publicly available exception”³ in the PDPA, which obviates the need to obtain consent and provide notification: see examples in the Key Concepts Guidelines at [12.63]. Although consent and notification are not required, section 18(a) of the PDPA may still operate to limit the collection, use or disclosure of such personal data to appropriate purposes. In determining the appropriateness of any particular purpose, considerations of the data subject’s objective expectation of privacy may conceivably be entertained. In this manner, the PDPA may provide similar protection to publicly available personal data as the common law. Personal data that was publicly available at the time it was collected can continue to be used or disclosed without the need for consent, even if the personal data is subsequently taken offline: see Key Concepts Guidelines at [12.61].

40 It may therefore be said that an interlocutor who wishes to prevent misuse of his private communication should look towards the new tort

³ As found in paragraphs 1(c) of the Second Schedule, 1(c) of the Third Schedule, and 1(d) of the Fourth Schedule to the PDPA.

established in *Campbell* and *Douglas*, with an eye on the PDPA where the private information is in the nature of personal data. The same observations made in respect of the right to prevent intrusion upon seclusion may be reiterated here: a private claimant prosecuting his case in the civil courts can plead both the common law tort to prevent publication of private information as well as pursue a private claim based on breaches of the PDPA. This not only provides him with a potentially more comprehensive set of reliefs, but will also provide the courts with the opportunity to consider adopting into our case law the same common law right in *Campbell* and *Douglas*. The Commissioner does not have the *vires* to extend its jurisdiction in these directions when investigating into a complaint.

Personality rights

41 I deal with the final two of Prosser’s categories collectively, as both relate to the protection of one’s personality from misuse or abuse.

Right to prevent appropriation of identity (personality and publicity rights)

42 The right of publicity is the right of an individual to control the commercial exploitation of an individual’s fame or identity: see David Tan, *Image Rights and Data Protection*, NUS Law Working Paper Series 2017/010 (“**David Tan, Image Rights and Data Protection**”) at p. 4. This extends to his name, image, voice, signature, or any other distinguishing characteristic which identifies him, and as such are considered personal data. Unsurprisingly, the Key Concepts Guidelines at [5.10], similarly lists data that on its own can identify an individual as “unique identifiers”: eg full name, facial image and voice of an individual. Needless to say, there must be commercial value in these characteristics in order for the right to publicity to provide a remedy for financial loss suffered as a result of unauthorised use: see the exposition of the law in the

United States in relation to publicity rights in Tugendhat and Christie, *The Law of Privacy and the Media*, 2nd ed. by Mark Warby QC, Nicole Moreham & Iain Christie, eds., (Oxford: OUP, 2011) at [3.110] – [3.114].

43 The right of publicity may be protected under intellectual property law, specifically, the law of passing off. Individuals may bring a cause of action under the tort of passing off to prevent false and unauthorised celebrity endorsements of goods and services. In the case of *Irvine v. Talksport Ltd* [2002] 1 WLR 2355 (“*Irvine*”), the English High Court acknowledged the expansion of the law of passing off to include cases of false endorsement. Insofar as an individual acquires a valuable reputation or goodwill, the law of passing off will protect it from unlicensed use by other parties. However, the claimant must be able to prove two interrelated facts: (i) at the material time, the claimant had significant reputation or goodwill, and (ii) the actions of the defendant gave rise to a false message which would be understood by a not insignificant section of his market that his goods have been endorsed, recommended or approved of by the claimant: *Irvine* at [46].

44 Given that there is a right of private action under the PDPA, it has been commented that the PDPA confers an “*incidental personality right*” on the individual, similar to the right of publicity: David Tan, *Image Rights and Data Protection* at p. 1. Whether the PDPA effectively creates a right of publicity regime in Singapore is open to debate. This and other pertinent issues are detailed in two articles and I can do no better than to refer the interested student to these commentaries: (a) David Tan, *Image Rights and Data Protection*; and (b) Gilbert Leong, Foo Maw Juin & Kenneth Fok, “Protecting the Right of Publicity under the PDPA” [2017] PDP Digest 293 (“**Gilbert Leong et al., Protecting the Right of Publicity under the PDPA**”).

Right to prevent false publicity (defamation and malicious falsehood)

45 The tort of false light publicity has been described as protecting interests similar to reputation, whilst having the same overtones of mental distress as in defamation: Prosser, *Privacy* at p. 400. At the heart of this false light tort is the need to protect the reputation of the person. Reputation is protected by English law in a number of ways, including malicious falsehood, passing off, and defamation. In *Tolley v. JS Fry & Sons Ltd* [1931] AC 333 (“*Tolley*”), an amateur golfer, who was depicted without his knowledge or consent in a newspaper advertisement for a Fry’s chocolate bar, sued in defamation arguing that the advertisement implied that he had compromised his reputation and status as an amateur golfer. Ultimately the House of Lords held in favour of the amateur golfer for defamation.

46 In Singapore, there has not been any express recognition of a tort of false light publicity, nor any indication that the PDPA was formulated to encompass such a tort. If the case of *Chiam See Tong v. Xin Zhang Jiang Restaurant Pte Ltd* [1995] 1 SLR(R) 856 (“*Chiam See Tong*”) is taken to set any precedent, it would be that any such rights are likely to be found in the areas of the law of defamation. In *Chiam See Tong*, the plaintiff successfully sued in defamation for damages and an injunction when a photograph taken of him at a restaurant for a charity fund raiser was subsequently used by the defendant as advertisements. It was held that to the ordinary reader, the photograph suggested that the plaintiff had consented to publicise the restaurant⁴.

⁴ If *Irvine* is followed in Singapore, a plaintiff in a similar case in Singapore may be able to sue both under the tort of defamation and passing off.

47 Recently, the English Court of Appeal in *Prince Moulay Hicham Ben Abdullah Al Alaoui of Morocco v. Elaph Publishing Ltd* [2017] 4 WLR 28 held that a data protection claim could be linked to a defamation claim for the reason that they were different causes of action which were directed to protecting different aspects of the right to private life, and the relevant provisions of the UK Data Protection Act 1998 included the aim of protection from being subjected unfairly and unlawfully to distress: at [43]. It would be too much of an extrapolation to read into this case – which was essentially an interlocutory appeal dealing with the issue of whether amendments to pleadings ought to be permitted – anything beyond the proposition that these are parallel remedies which the plaintiff may legitimately pursue.

48 It is in the area of personality rights that the area of overlap between the PDPA and common law rights is the greatest, since both operate on information that is essentially personal data. This is also the area where the contours between any common law right – this area of law is more developed in the United States than in the rest of the common law world – and statutory rights under the PDPA have yet to come under judicial scrutiny in Singapore. Based on the available commentary, the following observations may be made.

49 It has been observed that an individual may not have recourse under the PDPA, if the personal data is found in a publicly available space, even where an individual's fame has been commercially exploited: see David Tan, *Image Rights and Data Protection* at p. 15, and Gilbert Leong et al., *Protecting the Right of Publicity under the PDPA* at p. 297. It has also been pointed out that the definition of “personal data” does not adequately deal with the “*associative value*” that celebrities bring to products and services: David Tan, *Image Rights and Data Protection* at p. 4. Consequently, one may draw the conclusion that private action under the PDPA will probably have limited chance of

successfully preventing the classical scenario in which celebrities seek to prevent misuse or abuse of their personality when their identity is taken from a publicly available source: see *Tolley* and *Chiam See Tong*.

50 Private individuals are likely to have more success in relying on the PDPA to prevent misuse or abuse of their identity on the basis of use or disclosure without consent. But these are not what the cases on publicity rights thus far deal with. Perhaps the PDPA and the right of publicity are means to different ends – while the right of publicity seeks to protect the commercial value of the name or image of the individual, the PDPA seeks to hold organisations accountable for the proper and respectful handling of personal data, by imposing a standard of conduct that permits reasonable use, processing or disclosure while preventing misuse or abuse of personal data. This distinction may, in future, guide the Commissioner’s exercise of discretion when considering whether to commence investigations into complaints with personality rights undertones.

51 To be clear, while I have mentioned some causes of action above which may not as yet be recognised by the Singapore courts, I would exercise my discretion under section 50(3) to suspend, discontinue or refuse to conduct investigations where I believe there is a more appropriate cause of action which is recognised under Singapore law. But it is necessary to emphasise that our laws provide existing options to protect the privacy of an individual and this is an area that is expected to evolve. The PDPA deals with informational privacy and it would be a mistake to distort it in order to address privacy issues that it was not meant to address. Maintaining a macro perspective is necessary for the law in this area to develop.

The Commissioner's exercise of discretionary investigative powers in this case

52 It is against this backdrop of common law and statutory torts that collectively protect privacy rights that I explain the exercise of my discretion in this case.

I. The Commissioner's discretionary investigative powers

53 Section 50 of the PDPA provides me with the powers of investigation to determine whether an organisation is in breach of the PDPA. The powers of investigations are spelt out in the Ninth Schedule to the PDPA. Section 50(3) provides me a discretionary power to suspend, discontinue or refuse to conduct an investigation under specific circumstances. The relevant circumstance in this case is:

- (e) the Commission is of the opinion that --
 - (i) a complaint is frivolous or vexatious or is not made in good faith; or
 - (ii) any other circumstances warrant refusing to conduct, suspending or discontinuing the investigation.

54 In this case, the Complainant and the Organisation were engaged in civil proceedings before the District Courts. I understand that those proceedings have now been settled. The prime consideration is whether the subject matter of the present Complaint is better resolved through the judicial process or by an investigation into alleged breaches of the PDPA.

II. Action founded in the other areas of privacy

55 Having considered the complaint, I came to the view that the true nature of the Complainant's claim is for protection of his privacy which extends beyond protection of his personal data (which in the Complaint to the

Commission involves no more than the disclosure of his name), and thus this is not the appropriate office to investigate his claims. This is where the foregoing (somewhat lengthy) discussions about the interaction of the law on data protection and privacy becomes relevant.

56 This Complaint is the third complaint made by Complainant against the Organisation. The alleged infringement concerns the posting of a police report made by a member of the Organisation's staff containing the Complainant's name on Facebook, effectively suggesting that the Complainant was the culprit who carried out the online attacks and harassing acts. The Complainant is essentially alleging in this complaint that his reputation is affected by the Facebook post, because the disclosure of his name in the police report is akin to an accusation by the Organisation that the Complainant had been harassing the victim. All this takes place against the backdrop of a civil dispute between the Complainant and Organisation.

57 The immediate complaint raises issues relating to false light publicity that (as discussed above) lies within the domain of the law of defamation, which seems to be the branch of common law that is most appropriate for the development of rights to prevent false light publicity. The personal data that is disclosed is the Complainant's name. The rest of the police report details conduct that is attributed to him which may be of biographical significance.

58 While it is possible for me to investigate into whether the circumstances leading to the disclosure of the police report involved unreasonable conduct on the part of the Organisation, it is these same considerations that led me to conclude that addressing this one question would not be the most effective means of settling the dispute between the Complainant and the Organisation. As explained in *M Star Movers*, an organisation cannot be prevented from

defending itself on the same public forum that a complainant chooses to ventilate any dissatisfaction he may have against it. Disclosure of personal data may sometimes be necessary; and it is only when disclosure is a disproportionate response on the part of the organisation that the matter will be investigated under the PDPA. In order to determine whether to commence investigations, it becomes necessary to consider the allegations flowing between the complainant and the organisation, as well as the history of dissatisfaction between them. Given the history between the Complainant and the Organisation, resolving the dispute over the publication of the police report on Facebook is unlikely to settle the underlying dispute between them.

59 In the final analysis, the history of exchanges between the Complainant, the Sole Director and the Organisation disclose issues that can be better addressed before the courts. The legal issues that are potentially raised touch on the Complainant's expectations of privacy which, from our foregoing discussion, is protected by a framework of common law and statutory torts. I am unable to venture beyond the boundaries of the PDPA; the courts face no such constraint. The crux of the Complaint is that of publication of alleged defamatory remarks in a police report. A resolution of the underlying dispute relies on the framework of laws protecting privacy rights rather than the manner in which personal data is managed by the Organisation. Therefore, I did not think that this case was suitable for investigations under the PDPA and exercised my discretion under section 50(3)(e)(ii) of the PDPA to discontinue investigations.

60 The true nature of the Complaint revolves around the dispute between the Complainant and the Organisation over the Complainant's alleged online attacks and harassing acts. From the foregoing survey of our privacy laws, this is not an area that is exclusively within the domain of the PDPA. The POHA is

potentially relevant at least as an *existing* statutory tort; much more the potential of a common law right to privacy as in *C v. Holland* or *Jones v. Tsige*.

61 Indeed, it is specifically this category of cases that the PDPA was not meant to cover. In the parliamentary debates leading to the enactment of the PDPA, it was mentioned by Dr Yaacob Ibrahim, Minister for Information, Communications and the Arts (as he then was) that “[o]n Mr Zaqy Mohamad’s suggestion to cover cyber-bullying and other undesirable online behaviour, the Bill is concerned with regulating the management and the protection of personal data. It does not govern other actions of individuals online. This would be more appropriately addressed by others laws.” (emphasis added.) (Sing., *Parliamentary Debates*, vol. 89 (15 October 2012) (Assoc Prof Dr Yaacob Ibrahim) at p. 41). I can do no better than to echo the Minister’s statement. I do not think that the answer lies within the PDPA. On the precedent established in *Benber Dayao Yu v. Jacter Singh*, the answer today lies in sections 3 and 4 of the POHA: see [32] above.

62 Accordingly, for the reasons set forth above, I decided to exercise my discretion under section 50(3) of the PDPA to discontinue investigations into this Complaint and issue an advisory notice to the Organisation.

YEONG ZEE KIN
DEPUTY COMMISSIONER FOR
PERSONAL DATA PROTECTION
