

Technology, privacy and identity – a Hong Kong perspective

Please indicate the corresponding author.

Ji Lian Yap


School of Law
City University of Hong Kong
Tat Chee Avenue, Hong Kong
E-mail: jilyap@cityu.edu.hk
E-mail: yapjilian@yahoo.com.sg
*Corresponding author 

Rebecca Wong

Nottingham Law School
Nottingham Trent University
Burton Street, Nottingham
NG1 4BU, UK
E-mail: R.Wong@ntu.ac.uk

Abstract: This article explores the concepts of privacy and identity in Hong Kong in relation to the law relating to data protection. It first considers the notions of privacy and identity in the light of Hong Kong's socioeconomic situation and recent postcolonial heritage. It then highlights the importance of identity management and considers the distinctions and overlaps between identity management and privacy protection. With this conceptual framework in mind, the article then considers the various laws in Hong Kong pertaining to data protection, with a focus on the aspects relating to identity management. It observes that while there is some legal protection in respect of the data relating to an individual's identity, there are other priorities which may take precedence in determining the extent of identity management under the legal system in Hong Kong. Finally, recommendations are made as to how to improve identity management within the context of data protection in Hong Kong.

Please reduce keywords (maximum of ten words or phrases).

Keywords: privacy; identity; identity management; data protection; Hong Kong; HK; China; pseudonymous data; anonymity; new technologies; identity cards; copyright. 

Reference to this paper should be made as follows: Yap, J.L. and Wong, R. (xxxx) 'Technology, privacy and identity – a Hong Kong perspective', *Int. J. Intellectual Property Management*, Vol. X, No. Y, pp.000–000.

Biographical notes: Ji Lian Yap is a Teaching Fellow at the City University of Hong Kong, with teaching and research interests in commercial law, data protection and company law. She obtained her LLB from the National University of Singapore (1998) and her LLM (specialising in Commercial Law) from Cambridge University (2002). Her article, entitled 'The regulation of data privacy in Hong Kong', was published in *Cyberlaw, Security and Privacy* (2007).

Dr. Rebecca Wong is a Senior Lecturer in Law at Nottingham Law School, Nottingham Trent University, UK, with teaching and research interests in tort, intellectual property, data protection and cyberlaw. Her main areas of specialisation are in data protection and privacy. She holds an LLB (1998), MSc (2000), LLM (2001), PCHE (2004) and PhD (University of Sheffield, 2007) in data protection. She has written widely on privacy and data protection and her recent publications have included (2007) 'Data protection online: alternative approaches to sensitive data', *International Journal of Commercial Law and Technology*, Vol. 2, No. 1, pp.9–16 (reprinted in the *Journal of Internet Law*, March 2007 and *ICFAI Cyberlaw*, May 2007) and (2006) 'Demystifying clickstream data: a European and US perspective', *Emory International Law Review*, Vol. 20, No. 2, pp.563–590.

1 Introduction

Hong Kong is famous as a crowded city. Being a fairly mountainous place, livable space is relatively scarce and most humans live in close contact with one another. In laymen's eyes, privacy may thus be viewed as a luxury that one cannot always afford, rather than an absolute right that is automatically available to all. It is in this context that the ideas of privacy and identity management are examined in this article. What is the relationship between identity management and privacy protection, and how do these notions apply to the unique socio-economic landscape of Hong Kong? This article considers these questions, as a backdrop for an examination of the data protection framework in Hong Kong. To what extent is the notion of identity management promoted under the data protection laws in Hong Kong? What is the position of identity management (and indeed individual privacy protection) in relation to other socio-economic goals in Hong Kong? This article seeks to explore these questions, and ends with some recommendations as to how to improve identity management within the context of data protection in Hong Kong.

2 The concepts of privacy and identity management

2.1 Privacy

Hong Kong was a British colony until 1997, during which she was returned to China. It is now administered as one of the Special Administrative Regions of China. Culturally, Hong Kong retains strong Chinese roots, with the celebration of many Chinese festivals and with the majority of the population having the Cantonese dialect as their first language. Nonetheless, Hong Kong is an international financial centre with a cosmopolitan outlook. It seeks to be 'Asia's World City'. This slogan best embodies the dual nature of Hong Kong as an international city with a strong Asian focus. The concept of privacy in Hong Kong must thus be viewed in the light of this cross-cultural background.

The relationship between Hong Kong and China is governed by the Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China ('Basic Law'). This is basically a constitution-like document that sets out the relationship between the central Chinese authorities and Hong Kong. It also embodies certain

fundamental rights of Hong Kong residents, including Articles 28 (relating to personal privacy), 29 (relating to territorial privacy) and 30 (relating to privacy of communication). Notions of privacy are thus recognised under the Basic Law.

However, this must be viewed against the realities of Hong Kong's socio-economic landscape as an East Asian financial centre. One aspect of this is the crowded nature of Hong Kong which serves as a practical limit on the amount of territorial privacy that an individual may have. Another aspect is the importance of Confucian values in China as a whole.¹ Social harmony, resulting from every individual knowing his place in the social order and fulfilling his part, is a key theme in Confucianism. While not expressly against individual privacy, Confucianism does emphasise the importance of overall societal good. Thus the significance of privacy as a goal in itself is tempered to some extent by traditional Chinese viewpoint which places greater emphasis on other values.

Finally, it must be born in mind that Hong Kong is a very much pragmatic business society. One of the key reasons why laws promoting privacy have been adopted in Hong Kong is that Hong Kong may retain its place as a key financial centre. For example, in the report by the Law Reform Commission of Hong Kong on 'Reform of the Law relating to the Protection of Personal Data' (August 1994) it is stated as follows:

"If Hong Kong is to retain its status as an international trading centre, it is vital that it participates in the burgeoning international exchange of personal data. Increasingly, its capacity to do so will depend on its satisfying other countries that it offers an adequate level of legal recognition of the data protection principles."²

Therefore, we can see from this that the significance of privacy recognised not so much as an end in itself, but as one of the means by which the legal infrastructure of Hong Kong may be built to ensure its credibility as an international trading centre.

2.2 *Identity*

"Unlike a drop of water which loses its identity when it joins the ocean, man does not lose his being in the society in which he lives. Man's life is independent. He is born not for the development of the society alone, but for the development of his self." B.R. Ambedkar³

Identity is a multi-faceted concept. At its most basic level, it embodies the idea of the self as an entity as distinct from others. In this sense it is therefore a relative concept. The idea of identity can be expanded to take the form of group identity, focusing on the characteristics that distinguish one group from another. On a broader scale, it also encompasses the ideas of corporate identity or even national identity. Thus, what constitutes 'identity' can encompass a wide variety of factors, including one's race, tastes and orientation. The line between a factor constituting 'identity' and a mere attribute is of course a blurred one.

The concept of identity is one that is loaded with significance. A strong sense of identity carries with it ideas of personal pride. Identification with a group can bring with it feelings of collectiveness and community. In Hong Kong, following the handover in 1997, residents have to accept being identified not only as Hong Kong people, but also people of Mainland China.⁴

On a more prosaic level, a discussion of identity in Hong Kong would be incomplete without mention of the Hong Kong identity card ('ID card'). Residents in Hong Kong are required to register for an identity card, except those who are excluded or exempted under the Registration of Persons Ordinance and its regulations. ID cards can be used for immigration purposes, as well as for borrowing library books. In addition, ID card holders can store in their identity cards a personal e-Cert issued by the Hong Kong Post Certification Authority. The e-Cert may be seen as the users' online identity card. The e-Cert may be used for a whole host of public and commercial purposes, including electronic banking and trading, secured e-mail, government services and online entertainment.⁵ The legal framework with regard to ID card numbers will be considered later in this article.

2.3 Identity management

Proper identity management ensures that particulars constituting the identity of an individual are not stolen, abused or misused. An obvious example of this is the prevention of identity theft. It also involves ensuring that only selected individuals are allowed access to computer systems and databases. The primary driving force behind identity management initiatives is the promotion of trust. Users must be assured that the information that they give online is private and confidential. A strong framework for identity management is required so that there is sufficient confidence in e-commerce and other online transactions. Companies and governments need to ensure that access to their various systems and databases is confined only to authorised persons. This issue is particularly important in the context of the availability of inter-government department access to separate department databases, particularly with the increasing use of computers in governmental procedures. The preservation of control over information and systems can thus be seen to be one of the cornerstones of identity management.

Closely linked to the concept of identity management is the idea of transparency. The fact that one can remain anonymous on the web encourages creativity and free speech. In the world of e-commerce, trading partners may not be particularly concerned about the identity of whom they are trading with, so long each side is able to fulfil their respective sides of the bargain. However, the problem with anonymity is that it makes for lack of transparency and accountability. This in turn results in a tempting environment for activities such as money-laundering and terrorism financing.

2.4 The intersection between identity management and the privacy protection

The question then is whether the concept of identity management is synonymous with privacy protection. To address this question, we first have to consider the connection between identity and privacy. As can be seen from the discussion above, an individual's identity is essentially a positive concept that is concerned with self-definition in contrast to others. In contrast, the idea of privacy can be seen as largely a negative concept, namely the absence of interference with one's person, territory, data or communication. It has been said that "privacy is most appreciated in its absence, not its presence" (Chadwick, 2006). Generally, it is fair to say that the concealment of one's identity by means of anonymity or the use of pseudonyms would give more privacy. An individual's

privacy is inextricably connected with self, and therefore the concealment of self-identity would result in greater individual privacy. It would thus follow that better identity management would generally lead to greater privacy.

However, privacy is clearly a far broader concept than identity. The Australian Law Reform Commission has identified four privacy interests,⁶ namely:

- 1 the interest of the person in controlling the information held by others about him, or ‘information privacy’
- 2 the interest in controlling entry to the ‘personal place’ or ‘territorial privacy’
- 3 the interest in freedom from interference with one’s person or ‘personal privacy’
- 4 the interest in freedom from surveillance and from interception of one’s communications, or ‘communications and surveillance privacy’.

The first privacy interest (‘information privacy’) clearly includes the control of information regarding an individual’s identity. Similarly, protection of the fourth privacy interest (‘communications and surveillance privacy’) incorporates privacy with regard to one’s identity in one’s daily life and communications.

However, ‘territorial privacy’ and ‘personal privacy’ are concerned with the preservation of individual physical integrity, and are not so much concerned with individual identity as tangible spatial autonomy. Especially in a crowded city, it is entirely possible for one to be largely unidentified and anonymous in daily transactions as ‘one of a crowd’ while still having limited personal or territorial privacy.

The interplay between privacy and identification was illustrated in the Hong Kong Court of Appeal case of *Eastweek Publisher Ltd v Privacy Commissioner for Personal Data* (2000) 1 HKC 692. The applicants in this case (Eastweek Publishers) published a popular magazine called ‘Eastweek’. An article in September 1997 involved photographs of various women in public, taken without their knowledge or consent. None of the women featured in the report were fully named. One of the photographed women then complained to the Hong Kong Privacy Commissioner that she was upset by the negative comments made about her attire in the magazine.

At the Court of Appeal, Ribeiro JA expressed sympathy for the complainant and observed that she ‘would be entirely justified in regarding the article and the photograph as *an unfair and impertinent intrusion into her sphere of personal privacy*’. However the majority of the Court of Appeal concluded that there had been no contravention of the Data Protection Principles in the Personal Data (Privacy) Ordinance (Cap. 486) (‘PDPO’) as Eastweek was indifferent to the identity of the complainant. The case also illustrates the point that identity is a matter of perspective. The fact that the complainant in the photograph might have been identified by her friends was not sufficient for the majority of the Court of Appeal, which took the view that the crucial factor was whether the data user (Eastweek) was concerned with the identity of the women photographed. The further legal ramifications of this decision will be considered later in this article. However, it suffices to say here that this case shows how one may be regarded as insufficiently identified, and yet have one’s privacy undeniably and publicly invaded.

3 Legal framework

3.1 Overview of the personal data (privacy) ordinance

Having considered the conceptual overlaps and distinctions between privacy protection and identity management, we now turn to consider whether the current legal framework in Hong Kong sufficiently provides for and promotes identity management. The focus of this paper is personal data protection.

The primary piece legislation in Hong Kong in this regard is the PDPO, which came into effect in 1996. As stated in its long title, this is an Ordinance to protect the privacy of individuals in relation to personal data. The core of the PDPO is a set of Data Protection Principles, set out in Schedule 1 of the Ordinance. These relate to the purpose and manner of collection⁷ of personal data, the accuracy and duration of retention of personal data,⁸ the use⁹ and security¹⁰ of and access¹¹ to personal data. These principles must not be contravened¹² by data users¹³ unless expressly allowed under the Ordinance.¹⁴

The PDPO also provides for the establishment¹⁵ of the Privacy Commissioner for Personal Data ('PCPD'). The functions of the PCPD are (amongst others) to monitor and supervise compliance with the PDPO.¹⁶ The PCPD is empowered to issue Codes of Practice.¹⁷ He maintains a Register of Data Users,¹⁸ conducts inspections, handles complaints and carries out investigations¹⁹ in connection with the PDPO.²⁰

Various offences are stipulated under the PDPO.²¹ In addition, an individual who suffers damage (including injury to feelings) by a contravention of the PDPO may claim compensation from the data user.²² However, the efficacy of this right is somewhat watered down by the fact that it is defence to show that the data user had taken such care as was reasonably required to avoid the contravention concerned.²³ In addition, it has been pointed out that a further hurdle is that individuals have to hire their own lawyers as the PCPD cannot assist in litigation.²⁴

The crux of scope of the PDPO is the definition of 'personal data', which is defined in Section 2 of the PDPO as:

"any data-

- (a) relating directly or indirectly to a living individual;
- (b) from which it is *practicable for the identity of the individual to be directly or indirectly ascertained*; and
- (c) in a form in which access to or processing of the data is practicable."
(emphasis added)

'Data' is in turn defined in Section 2²⁵ of the PDPO to include a 'personal identifier' 'Personal identifier' is defined in the same section as:

"an identifier-

- (a) that is assigned to an individual by a data user for the purpose of the operations of the user; and
- (b) that *uniquely identifies that individual* in relation to the data user, but does not include an individual's name used to identify that individual."
(emphasis added)

It can be seen (particularly from the italicised portions of the respective definitions) that the general notion of 'personal data' in the PDPO recognises to some extent the concept of identity management. However, some ambiguities exist. For example, what data might

Please indicate where the closing quotation mark should be placed.

‘uniquely’ identify an individual in order to constitute a ‘personal identifier’ is a question of degree. On the one hand, a Hong Kong ID card number should clearly satisfy this requirement. On the other hand, a written description of a man called David Lee, aged 30 and (living) in Tsimshatsui probably would not. However hypothetically speaking, what if it was somehow known to the data user that there was only one person fitting this description? What if the area in question was reduced to one street, or one apartment block? It is thus a question of fact in the individual case as to what constitutes ‘personal identifiers’ under the PDPO.

Another ambiguity lies in limb (b) of the definition of ‘personal data’, which stipulates that in order for data to constitute personal data, it must be data ‘from which it is practicable for the identity of the individual to be directly or indirectly ascertained’. It is not clear whose point of view such identification is to be ascertained. Would it be sufficient if the ‘data user’²⁸ is able to ascertain the identity of the individual? Or is it sufficient if any person (not necessarily the data user) can do so? The significance of this question is of interest in the context of pseudonymous data, which will be considered in the next section.

In addition to the general provision as considered above, several specific provisions of the Ordinance reflect the notion of identity management. For example, a report published by the PCPD following an inspection or investigation shall be so framed as to prevent the identity of any individual being ascertained from it.²⁹ In addition, a data user shall refuse to comply with a data access request if the data user cannot comply with the request without disclosing personal data of which any other individual is the data subject, unless the data user is satisfied that the other individual has consented to the disclosure.³⁰

Thus, it appears that the provisions of the PDPO do recognise, to some extent, the importance of identity management. However, a specific issue with regard to identity management is the extent to which pseudonymous data is protected. The next section considers the extent of such protection offered under the PDPO.

3.2 Pseudonymous data

The concept of pseudonymous data derives from the use of pseudonyms that mask the true identity of the data subject. There are many examples of pseudonyms online, for example, e-mail addresses. People may use pseudonyms in order to maintain a degree of anonymity in their online transactions, thus retaining for themselves a greater degree of privacy.

If there is true and complete anonymity in the sense that the individual behind the data cannot be traced by any means, then there would be no identifiable individual to protect. Such information would not fall within the scope of ‘personal data’³¹ under the PDPO.

The position is less clear when it comes to pseudonymous data and it would depend on the particular case. For example, if the individual is well-known and goes by a public pseudonym, it is arguable that such pseudonymous data would constitute data relating directly to an individual ‘from which it is practicable for the identity of the individual to be directly or indirectly ascertained’,³² thus falling within the definition of ‘personal data’ in the PDPO. In contrast, if it is impossible for the pseudonym to be linked to any individual, that is akin to anonymity and would not be within the scope of the PDPO.

What of pseudonymous data that the data user is able to link to an individual, though the general public would not be able to do so? The key issue is whether limb (b) of the definition of 'personal data' is satisfied, namely, whether it is 'practicable for the identity of the individual to be directly or indirectly ascertained'. As mentioned above, this definition does not explicitly clarify whether it is sufficient that the identity of the individual is ascertainable only by a data user and no one else. However, it is submitted that data should constitute 'personal data' if the data user alone is able to ascertain the identity of the individual. To impose more stringent requirements in limb (b) of the definition of 'personal data' would be to read in extra requirements into the statute, and limit the efficacy of the PDPO as a means of privacy protection.

IP addresses are regarded as a form of pseudonymous data, insofar as they pertain to a particular computer. However it is unclear whether IP addresses would fall within the definition of 'personal data' under the PDPO. While IP addresses relate to a particular computer, various individuals may use that computer, possibly without the ISP account holder's permission. This problem is exacerbated by the advent of wireless networks which may be accessed without authorisation.³³ The problem is one of accurate attribution, in the sense the ISP account holder is not necessarily the person using the computer at all times. On this basis, it is arguable that IP addresses relate to a particular computer, rather than an individual, and are thus not 'personal data' within the PDPO. The counter-argument to this is that IP addresses do relate to the ISP account holder, and would thus constitute 'personal data' on a literal reading of the definition, despite the fact that the account holder may not be the actual user at the relevant time.

The office of the PCPD has previously expressed the view that an IP address alone does not satisfy the definition of 'personal data' in the PDPO, but that if the IP address is combined with identifying particulars of an individual, from which it is practicable for the identity of the individual to be ascertained, the IP address may become part of the 'personal data'.³⁴ However, this view still does not address the question of who must be able to ascertain the identity of the individual in order for the data to constitute 'personal data'.³⁵ It is also worth noting the views of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data ('Working Party') set up under the European Union Data Protection Directive 95/46/EC ('EU Data Protection Directive').³⁶ The Working Party has generally considered IP addresses as data relating to an identifiable person, thus constituting 'personal data' within the definition in Article 2(a) of the EU Data Protection Directive.³⁷ Nonetheless, the ambiguities with regard to IP addresses reveal the difficulties in the application of the technologically neutral tones of the PDPO to online technologies.

3.3 ID card numbers

The ID card number is a form of pseudonymous data that is ubiquitous in Hong Kong. Whilst in other jurisdictions the proposed introduction of ID cards has met with criticism and scepticism, in Hong Kong they have long been accepted as part of daily life. However, the use of ID cards should give rise to some degree of concern over privacy invasion. This is exacerbated by the recent introduction of the e-Cert (as mentioned above), which allows a wide variety of transactions to be carried out with the ID card.³⁸

ID card numbers clearly fall within the definition of 'personal identifier'²⁸ in the PDPO. Indeed, it was noted in the publication by the PCPD entitled 'Your Identity Card Number and Your Privacy'³⁹ that 'by far the most commonly used personal identifier in

Hong Kong is the ID card number'. 'Data'²⁸ is defined in the PDPO to include 'personal identifiers'. The issue then is whether ID card numbers constitute 'personal data'²⁸ under the PDPO, in particular, whether ID card numbers are data 'from which it is practicable for the identity of the individual to be directly or indirectly ascertained'.⁴⁰ Pertinent to this issue is the question (earlier discussed) of whose point of view the identification of the individual is to be ascertained, in order for data to constitute 'personal data'. Whether an ID card number is 'personal data' under the PDPO would depend on the facts of each case. A data user in possession of an ID card number alone but with no information as to the name of the person to whom the number has been assigned, might not be able to ascertain the identity of the individual. However, if the view is taken that data can be regarded as 'personal data' as long as the individual's identity can be ascertained by any person (not necessarily the data user), then the ID card numbers should still fall within the definition of 'personal data'. If ID card numbers constitute 'personal data' under the PDPO, then the Data Protection Principles therein would apply.

In addition to the general provisions of the PDPO, a Code of Practice on ID Card Numbers and other Personal Identifiers (the 'ID Card Numbers Code')⁴¹ has been issued by the PCPD. As stated in the accompanying Compliance Guide for Data Users, the Code gives practical guidance to data users on the application of the PDPO to the collection, accuracy, retention, use and security of ID card numbers and other personal identifiers (such as passport numbers, employee numbers, patient numbers and examination candidate numbers). The Code provides (among other things) that no data user may compulsorily require an individual to furnish his ID card number unless authorised by law, and that the data user should consider whether there are less privacy-intrusive alternatives to the collection of such numbers.⁴² Non-compliance with the ID Card Numbers Code does not of itself render the data user liable to any civil or criminal proceedings.⁴³ However, a breach of the ID Card Numbers Code would give rise to a presumption against the data user in legal proceedings under the PDPO.⁴⁴

For completeness, it must also be noted that the Registration of Persons Ordinance ('RPO') provides some further protection. Pursuant to the RPO, particulars furnished to a registration officer may be used only for the purpose of enabling the Commissioner⁴⁵ to issue ID cards and to keep records on such particulars. Moreover, these records may be used only for the following purposes, namely:

- “(i) enabling verification of identity of individuals by public officers in discharge of their official duties;
- (ii) enabling verification of identity of individuals for *any other lawful purposes*; or
- (iii) such purposes as may be authorized, permitted or required by or under any Ordinance.”⁴⁶ (emphasis added)

The phrase 'lawful purpose' is not defined in the RPO and its meaning is unclear. For example, if the records are used to verify the identity of an individual in order for a private civil claim to be made against him, is that a 'lawful purpose'? We can only infer that what amounts to a 'lawful purpose' should be broader than what is specified in paragraphs (i) or (iii). However, the potentially broad interpretation that could be given to the phrase 'lawful purpose' compromises the protection for particulars of individuals in records maintained by the Commissioner.

A similar problem may be observed in Section 12 of the RPO. Pursuant to that section, any person who, without lawful authority or reasonable excuse, gains access to, uses or discloses any records kept by the Commissioner shall be guilty of an offence.⁴⁷ The RPO does not provide further details on what would constitute a ‘reasonable excuse’ or ‘lawful authority’ under this section.⁴⁸ In particular, the question of who would have the power to confer ‘lawful authority’ on the otherwise offending individual is left unanswered.⁴⁹

Having considered the various relevant legislative provisions, we can now turn to several judicial decisions that have affected the scope of application of the PDPO, particularly in relation to the issue of identity management.

3.4 *Personal data collection*

In the case of *Eastweek Publisher Ltd v Privacy Commissioner for Personal Data* (the facts of which are discussed above), the majority of the Court of Appeal found that it was of the essence to the act of personal data collection under the PDPO that the data user must be compiling information about an identified person or about a person whom the data user intends or seeks to identify. As this element was absent on the facts, it was found that there had not been an act of personal data collection.

It is not an express requirement of the PDPO that personal data collection necessarily involves the data user having identified or intending to identify the data subject. The majority of the Court of Appeal has thus narrowly interpreted the notion of personal data collection in the PDPO. Consequently, this decision narrows the scope of identity management under the framework of the PDPO. Unless the data user had identified or was intending to identify the data subject, the act of data collection would not fall within the scope of the PDPO, even if the identity of the individual is clearly discernable from the information (as it was in this case with the photograph).⁵⁰

3.5 *Applications to court relating to identity of online copyright infringers*

The interplay between privacy and identity has been seen in several recent Hong Kong cases involving applications by members of the recording industry against Internet Service Providers (‘ISPs’) for the disclosure of information on the identity of internet subscribers who were allegedly involved in infringement of the plaintiffs’ copyright.

The Court of First Instance case of *Cinopoly Records Co Ltd & Others v Hong Kong Broadband Network Ltd & Others*⁵¹ [‘Cinopoly 1’] before Deputy Judge Poon was described by the learned judge as ‘the first of its kind ever brought in Hong Kong’.⁵² In that case, seven leading music producers brought an action against four ISPs for the names, Hong Kong ID card numbers and addresses of 22 alleged online copyright infringers.

That case was swiftly followed by another similar application in *Cinopoly Records Company Limited v Hong Kong Broadband Network Limited* [HCMP 943/2006] [‘Cinopoly 2’] for the disclosure of the full names, postal addresses and ID card numbers of 49 internet account subscribers. In both these case, the relief sought by the music producers was granted.⁵³

These issues in these cases are significant because, as Deputy Judge Poon put it, they ‘(bring) into focus the very fine and delicate balance that the court needs to strike between the administration of justice and protection of privacy relating to personal data’.⁵²

These cases involved alleged copyright infringement using ‘Peer-to-Peer’ (‘P2P’) technology.⁵⁴ The Court noted the widespread use of such P2P software in Hong Kong, and the deleterious consequences that such usage for the music industry. In particular, the Court noted that the extent of copyright violation was so extreme that the plaintiff’s viable existence was very much at stake.

The Court then emphasised the nub of the problem which was the ‘cloak of anonymity’⁵⁵ that infringer could hide his identity behind in the use of P2P software. As the parties who were infringing the copyright could not be identified, copyright holders were left in a helpless position.

However, this ‘cloak of anonymity’⁵⁵ could be pierced with the help of information from the ISPs, matching the IP address at the relevant time, with the ISP’s records of its subscribers’ particulars including their names, ID card numbers and postal addresses. The court stressed that this was the only way that the plaintiffs could proceed against the alleged copyright infringers.

The plaintiffs thus sought *Norwich Pharmacal* discovery against the ISPs.⁵⁶ The Court discussed the essential elements for the granting of such relief, and concluded that each of these elements had been satisfied. The first element was that serious tortious or wrongful activities had been committed. The Court found that this was the case as there had been copyright infringement under the Copyright Ordinance.⁵⁷ In particular, the Court noted that some of the downloaded songs had not yet been made commercially available.

The second element was whether the subscribers could reasonably be assumed to be the copyright infringers. The Court noted that there could be multiple users to an internet account and thus the subscriber might not have been the individual who wrongfully downloaded the material. However, the Court took the view that it was reasonable to infer that the subscriber could have consented or authorised others to use his internet account to download the material. The third element, relating to the ISP’s innocent involvement in the uploading, was also clearly established.

The Court then considered what it termed to be ‘the most important question in this action, namely, how to strike the balance between the administration of justice and protection of privacy relating to personal data’.⁵⁸ In carrying out this balancing exercise, the Court had to consider the application of the provisions of the PDPO. The information sought by the plaintiffs was clearly ‘personal data’ within the definition in Section 2 of the PDPO.⁵⁹ The issue then was whether *Norwich Pharmacal* relief was available in such circumstances.

The relevant Data Protection Principle was Principle 3, pursuant to which personal data should not be used for any purpose other than the purpose for which the data were to be used at the time of data collection, or a purpose directly related thereto.

However personal data is exempt from Principle 3 if the use of the data is for the purpose of ‘prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, or dishonesty or malpractice, by persons’⁶⁰ and if the application of Principle 3 ‘would be likely to prejudice’⁶¹ such purpose. The Court found that the phrase ‘unlawful or seriously improper conduct’ covered tortious conduct, including copyright infringement. Thus the exemption from Data Protection Principle 3 was applicable.

The Court reasoned that to hold otherwise would be to deprive a victim wronged by tortious conduct of *Norwich Pharmacal* relief when the information sought was personal data within the meaning of the PDPO. To quote Justice Poon:

“Norwich Pharmacal discovery is a well-established equitable relief. Nothing in the Ordinance...suggests that this entrenched relief is removed when the information sought is personal data within the meaning of the Ordinance. The Legislature could not have intended to alter the law by a sidewind.”⁶²

As mentioned above, *Cinepoly 1* was followed shortly after by another similar application which was granted in *Cinepoly 2*. However, in granting the application in *Cinepoly 2*, Judge Chan emphasised that each of the plaintiffs would only be entitled to the information of the identity of those uploaders who had infringed each of their respective copyrights. His Honour clarified that if there should be no infringement by any uploader of the copyright of any particular plaintiff, the information of that uploader should not be disclosed to that plaintiff as there was no justification for that disclosure.

Overall, these cases are instructive as an indication of the Hong Kong approach to the proper balance between data protection (an aspect of which includes identity management) on the one hand, and the protection of other competing interests. The anonymity that is afforded by P2P software clearly has its advantages. Users are free to download material without fear that their choices (and by implication their tastes, preferences and personal orientation) will be traced back to them. However, where such activity involves the committing of civil wrongs, the balance then swings to protect intangible property rights, such as copyright.⁶³

This approach is clearly set out in the ‘timely reminder’⁶⁴ issued by Justice Poon at the end of his judgment in *Cinepoly 1*:

“Some online copyright infringers may well think that they will never be caught because of the cloak of anonymity created by the P2P programs. They are wrong. And from now on, they should think twice. They can no longer hide behind the cloak of anonymity. The court can and will, upon a successful application, pull back the cloak and expose their true identity. *It is not an intrusion into their privacy.* It does not even lie in their mouths to say so. *For protection of privacy is never and cannot be sued as a shield to enable them to commit civil wrongs with impunity* (emphasis added).”⁶⁴

This is perhaps illustrative of the pragmatic approach towards the right to privacy in Hong Kong.⁶⁵ The decision in this case is clearly in favour of commercial interests, namely copyright protection. It contributes towards the building of a business-friendly legal infrastructure in Hong Kong. It can be inferred from this decision that weight will be given to the protection of commercial interests, as against the protection of confidentiality of one’s identity.⁶⁶

Identity management is an integral aspect of most information systems. To this end, the protection of identity is important from a commercial point of view. However, it can be seen from this case that privacy is merely one factor in the economic equation and may be displaced if other commercial interests are found to take precedent.

4 Recommendations

From the discussion above, it is clear that while there has been some tangential account taken of identity management in the formulation of Hong Kong’s laws on data protection, the particular issue of identity management has not been directly addressed. Having

discussed the importance of identity management in today's digital age (in particular the need to provide for integrity with regard to identity in order to promote trust), it is suggested that the theme of identity management requires and deserves to be addressed and emphasised as a specific factor in the ongoing development of Hong Kong's data protection regime.

Several recommendations flow from this overall point. Firstly, it is suggested that there be more emphasis on the collection and use of anonymous or pseudonymous data where identification of individuals is not required. This reiterates a view held by other writers.⁶⁷ Paragraph 1(c) of the Data Protection Principles in the PDPO provides that the data collected should be adequate but not excessive in relation to their intended purpose. However, the legislation should go further to specify that where identity is not required, only anonymous data be collected. If pseudonymous data would suffice without the actual identity of the individual being collected, it should then be specifically provided that the collection is restricted to such pseudonymous data. This approach is reflected in the data protection regimes of some other jurisdictions.⁶⁸ A hint of this can already be found in the ID Card Numbers Code (as discussed above), pursuant to which the data user should consider whether there are less privacy-intrusive alternatives to the collection of such numbers.

Secondly, it is suggested that the definition of 'personal data' in Section 2 of the PDPO be clarified as to who must be able to ascertain the identity of the individual in order for data to constitute 'personal data'. In this regard, reference can be made to the UK Data Protection Act ('UK DPA'). Pursuant to Section 1(1) thereof, 'personal data' means *data* which relate to a living individual who can be identified from those *data*, or from those *data* and other information which is in the possession of, or is likely to come into the possession of, the *data controller*.⁶⁹ It can be seen that, as regards data that has to be combined with other information in order for an individual to be identified, the relevant point of view is the data controller. In the context of the PDPO, the corresponding party would be the data user.⁷⁰ Such an approach would promote certainty as to the proper scope of 'personal data' under the PDPO. In contrast, a somewhat wider and looser formulation may also be observed in the European Union Data Protection Directive. Recital 26 thereof provides that 'to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person'. In order to increase the scope of 'personal data' and to fully meet the objective of the PDPO to protect privacy, it is suggested that the wider formulation in the EU Data Protection Directive is to be preferred. In addition, there appears to be no reason in principle why a determination of whether data is 'personal data' should be restricted only to information in the possession of the data controller.

It must finally be noted that identity management can only be brought to the forefront of data protection if there is awareness and education among businesses, technology developers and the general public with regard to this issue. In this regard, it is suggested that the PCPD take a pro-active role in the promotion of public awareness of identity management issues.

5 Conclusion

Throughout this paper we have considered the scope of identity management in the context of the data privacy regime in Hong Kong. Hong Kong holds a unique place in Asia, being a successful Chinese financial centre and also until 1997 a British colony. In the light of this history and culture, there are special nuances attached to the ideas of privacy and identity. The growing importance of identity management calls for special focus on it as a distinct issue in the context of data protection. Whilst ideas of identity management are to some degree encapsulated within the overall data privacy framework, there is still room for greater protection of information relating to an individual's identity. The first step is to recognise identity management as a specific factor that must be addressed directly, rather than tangentially, within the data protection framework. Identity management (and indeed privacy protection) are not absolute rights and will always jostle with other goals for precedence, as the *Cinepoly* cases illustrate. However, it is important that the concept of identity management be given greater recognition in Hong Kong, in order for there to be a robust and comprehensive legal infrastructure for the promotion of trust in this technological age.

Reference

Chadwick, P. (2006) 'The value of privacy', *EHRLR*, p.5.

Notes

- 1 According to an article in the South China Morning Post on 12 July 2007 entitled 'Communists dust off Confucius amid upheaval of rapid growth', Confucianism is 'fast catching up with communism as the mainland's rulers, businessmen and ordinary citizens turn back 2500 years to (Confucius') teachings to help them to cope with the economic and social changes wracking the country'.
- 2 Paragraph 5.7 of the Report by the Law Reform Commission of Hong Kong on 'Reform of the law relating to the protection of personal data' (August 1994).
- 3 B.R. Ambedkar (1891–1956) was an Indian scholar and political leader who fought against the system of Hindu untouchability and the caste system.
- 4 According to an article in the South China Morning Post on 13 June 2007, a survey conducted by the University of Hong Kong revealed that the number of Hong Kong teenagers identifying themselves as Chinese Hongkongers has risen in the last decade.
- 5 More information on the e-Cert can be found on the Hong Kong Post website at <http://www.hongkongpost.gov.hk/activity/smartid/index.html>. Internet addresses in this and all other references were last checked on 21 July 2007.
- 6 Paragraph 46 of the Australian Law Reform Commission, Privacy (Report No. 22) (1983).
- 7 Principle 1, Schedule 1, PDPO.
- 8 Principle 2, Schedule 1, PDPO.
- 9 Principle 3, Schedule 1, PDPO.
- 10 Principle 4, Schedule 1, PDPO.
- 11 Principle 6, Schedule 1, PDPO.
- 12 Section 4, PDPO.

- 13 'Data user' is defined in Section 2 of the PDPO as follows: 'data user', in relation to personal data, means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data.
- 14 Exemptions to the various requirements of the PDPO are set out in Part VIII thereof.
- 15 Section 5 of the PDPO.
- 16 Section 8 of the PDPO.
- 17 Part III of the PDPO.
- 18 Part IV of the PDPO.
- 19 Part VII of the PDPO.
- 20 Case notes on the complaints dealt with by the PCPD can be found on the PCPD's website at www.pcpd.org.hk.
- 21 Section 64 of the PDPO.
- 22 Section 66 of the PDPO.
- 23 Section 66(3) of the PDPO.
- 24 'Who let the cat out of the bag? Internet data leakage and its implications for privacy law and policy in Hong Kong' by Alana Maurushat, 36 *HKLJ* 7 (2006).
- 25 The full definition of 'data' in Section 2 of the PDPO is 'any representation of information (including an expression of opinion) in any document, and includes a personal identifier'.
- 26 Tsimshatsui is a busy commercial district in Hong Kong.
- 27 Example given by dissenting judge Wong JA in *Eastweek Publisher Ltd v Privacy Commissioner for Personal Data* (2000) 1 HKC 692.
- 28 As defined in Section 2 of the PDPO.
- 29 Section 48, PDPO.
- 30 Section 20, PDPO.
- 31 As defined in Section 2 of PDPO.
- 32 Limb (b) of the definition of 'personal data' under the PDPO.
- 33 This problem is discussed in 'Online piracy and the copyright challenge in Hong Kong' (a paper presented by Rebecca Ong in the 2006 LSPI Conference in Hamburg, Germany) in connection with the question of whether Hong Kong should follow the US model, under which information identifying alleged illegal file sharers can be obtained by a subpoena issued by a court clerk.
- 34 Press release from the PCPD on 15 March 2007 entitled 'Further response to the investigation report', relating to the result of an investigation of disclosure by an e-mail service provider of its account subscriber's personal data to the PRC law enforcement authorities. Available on PCPD's website <http://www.pcpd.org.hk>.
- 35 This issue is further discussed in Part 4 with regard to 'Recommendations', which includes a discussion of the respective positions under UK laws and European Union Directives.
- 36 A detailed comparison between the concept of 'personal data' as set out in the working party's opinion 4/2007 on the concept of personal data, and that as existing under PDPO in Hong Kong, is beyond the scope of the present article.
- 37 Example No. 15: dynamic IP addresses, in the working party's opinion 4/2007 on the concept of personal data.
- 38 Further information on the rules and procedures governing the e-cert can be found in the certification practice statement of the Postmaster General at http://www.hongkongpost.gov.hk/product/cps/ecert/img/cps_en22.pdf.
- 39 This can be found on the PDPO's website at <http://www.pcpd.org.hk>.
- 40 Limb (b) of the definition of 'personal data' in Section 2 of the PDPO.

- 41 The code and the compliance guidelines for data users can be found on the PCPD's website <http://www.pcpd.org.hk>.
- 42 Paragraph 2 of the ID Card Numbers Code.
- 43 Section 13(1) of the PDPO.
- 44 Section 13(2) of the PDPO.
- 45 'Commissioner' is defined in Section 2 of the RPO.
- 46 Section 9 of the RPO.
- 47 The full wording of Section 12 of the RPO is as follows: 'Any person who, without lawful authority or reasonable excuse, gains access to, stores, uses, discloses, erases, cancels or alters any record kept by the Commissioner on particulars furnished to a registration officer under this ordinance shall be guilty of an offence and shall be liable to a fine at level 5 and to imprisonment for two years'.
- 48 Section 30(1) of the Prevention of Bribery Ordinance (Cap. 201) makes it an offence to disclose 'without lawful authority or reasonable excuse' to any person the identity of any person who is the subject of an investigation or any details of such an investigation. This section was discussed in *Hall v ICAC* (1987) HKLR 210.
- 49 Other provisions that seek to offer some degree of protection to individual identity are Sections 10 and 11 of the PRO, which impose on registration officers a duty not to disclose photographs, fingerprints or particulars except in the circumstances specified therein.
- 50 It has been pointed out that a consequence of this narrow interpretation is that the mass collection of e-mail addresses or information on web-surfing behaviour, (where the data collector is not concerned with individual identity) would not be caught under the PDPO: Privacy and Anonymity, Raymond Wacks. 30 *HKLJ* 177 (2000).
- 51 (2006) 1 HKLRD 255.
- 52 (2006) 1 HKLRD 255 at p.259.
- 53 See 'Online piracy and the copyright challenge in Hong Kong' (a paper presented by Rebecca Ong in the 2006 LSPI Conference in Hamburg, Germany) for further discussion on *Cinepoly 1* and whether Hong Kong should follow the US model, under which information identifying alleged illegal file sharers can be obtained by a subpoena issued by a court clerk.
- 54 Judge Poon described a typical scenario: "A subscriber to an Internet Service Provider (ISP) stores music in the hard disc of his computer, either from a legitimate or illegitimate source. If he wishes to share his music stored in his computer, he uploads and posts it in the 'shared folders' in the P2P software. The 'shared folders' file can then be searched, assessed to and downloaded by other computers using the same software." (2006) 1 HKLRD 255 p.260.
- 55 (2006) 1 HKLRD 255 at p.261.
- 56 This was a form of equitable relief established in the case of *Norwich Pharmacal Co v Customs and Excise Commissioners* (1974) 4 AC 133.
- 57 Specifically, Sections 24(2), 26(2) and 32(2) of the Copyright Ordinance.
- 58 (2006) 1 HKLRD 255 at p.266.
- 59 On a separate note, in connection with the earlier discussion on IP addresses, it is interesting to note that the question of whether IP addresses themselves constitute 'personal data' under the PDPO was circumvented in this case, as the information sought was information gleaned using the IP addresses rather than the IP address itself.
- 60 Section 58(1)(d) of the PDPO.
- 61 Section 58(2) of the PDPO.
- 62 (2006) 1 HKLRD 255 at p.271.
- 63 For a discussion on the relationship between copyright and privacy, refer to 'IP, phone home: the uneasy relationship between copyright and privacy, illustrated in the laws of Hong Kong and Australia' by Graham Greenleaf. 32 *HKLJ* 35 (2002).
- 64 (2006) 1 HKLRD 255 at p.274.

- 65 For a European perspective, reference may be made to the opinion in case C-275/06 (*Productores de Musica de Espana Promusicae vs. Telefonica de Espana SAU*, in which the adviser to the European Court of Justice, Advocate General Juliane Kokott, considered that, in accordance with EU law, the ISPs are not obliged to reveal personal data in civil litigation cases.
- 66 Indeed, the Intellectual Property Department of the Hong Kong Government has released a consultation document to solicit views on whether legislative amendments should be made to allow a relatively quicker and inexpensive procedure for copyright owners to obtain from Internet Access Service Providers information disclosing the identity of online infringers. The results of this consultation are not yet known. Further details of this consultation paper can be found on the Intellectual Property Department's website www.ipd.gov.hk.
- 67 Professor Raymond Wacks in his book *Hong Kong Data Privacy Law* (Sweet and Maxwell Asia 2003) (paragraph 17.39) has suggested that an anonymity principle be added to Hong Kong's Data Protection Principles. It was also pointed out by Graham Greenleaf in 'IP phone home: the uneasy relationship between copyright and privacy, illustrated in the laws of Hong Kong and Australia' 32 *HKLJ* 35 (2002) that (unlike Australia), Hong Kong does not have such an 'anonymity requirement'.
- 68 Section 3a of the German Federal Data Protection Act provides that use is to be made of the possibilities for anonymisation and pseudonymisation, insofar as this is possible and the effort involved is reasonable in relation to the desired level of protection.
- 69 In Australia, National Privacy Principle 8 provides that wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.
- 70 'Data controller' is defined in Section 1(1) of the UK DPA as a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any *personal data* are, or are to be, *processed*.