SUBMISSION FOR PRIVACY COMMISSIONER PRIZE 2015-16

TOIPC 4: PERSONAL DATA PRIVACY AND PUBLICLY AVAILABLE INFORMATION

TITLE OF PAPER: CONTROL OR BEING CONTROLLED: ERASING PERSONAL DATA IN PUBLIC DOMAIN IN HONG KONG

Submitted by Chan Tsz Wai Michelle, LL.B. (Hons.), the University of Hong Kong

8 July 2016
Control or Being Controlled: Erasing Personal Data in Public Domain in Hong Kong*

Michelle Chan**

Contents

Introduction .............................................................................................................................................. 2
I. Understanding Privacy and Personal Information .............................................................................. 3
II. Where Are Our Privacy Laws Heading To? ...................................................................................... 6
   a. The English Law ....................................................................................................................... 6
   b. The European Approach ......................................................................................................... 8
   c. Reflections from the Do No Evil App and the David Webb cases in Hong Kong ............... 11
III. Implementing a Right to De-list in Hong Kong .............................................................................. 14
   a. Why it is important to discuss the possibility of introducing a right to de-list in Hong Kong . 14
   b. Understanding privacy as a right to control ............................................................................. 15
   c. The Proposal ............................................................................................................................... 15
      i. Reframing statutory definition of data user ........................................................................... 16
      ii. The three criteria approach ................................................................................................. 17
      iii. Reasonable efforts ................................................................................................................ 19
      iv. Balance between a right to de-list and freedom of expression ......................................... 20
      v. Defences and exemptions ..................................................................................................... 21
Conclusion ............................................................................................................................................ 24

---

*This article is amended from an article bearing the same title submitted for publication in the Hong Kong Journal of Legal Studies, Volume 10. Publication has been accepted by the editors.

** LL.B. (Hons.) HKU. The author would like to express her sincerest gratitude to Dr. Marcelo Thompson for his patience, guidance, insights and comments.
Introduction

Advancement of information technology has altered the way information is collected, stored and disseminated. With computerisation and emergence of online intermediaries, access to public records is made far more convenient and flexible. Various search engines, websites and applications gather public records of citizens, organise them, and make them publicly available on their platforms. Obtaining information of target persons becomes as easy as a click on the finger. While these online intermediaries act as conduits for communication and facilitate free flow of information\(^1\), they may also lead to unwanted publicity of information, particularly when the information is considered to be personal.

It was against this background that the Google Spain case\(^2\) caught the media attention and sparked a fierce debate worldwide about whether we should have a ‘right to be forgotten’. Briefly, the case concerns a request from a Spanish citizen to Google Spain to remove links to newspapers announcement in 1998 which contains his name. The case went all up to the European Court of Justice. The Court decided that Google should delete the hyperlinks at issue. The worldwide attention of the case reflects a common fear of people living in an information age: once our personal data is exposed in a public online environment, do we lose our control over it?

The Google Spain case was widely discussed in legal communities. However, most of the articles focus on analysing the judgment and explaining the concept of the “right to be forgotten”. The crucial question of whether countries outside the European Union should adopt a right to be forgotten is, surprisingly, scarcely discussed by academics in countries apart from the United States. In light of the real concern of privacy in public in the era of digitalisation, a more open discussion about the extent of control citizens can exert over their data in the public domain is called for.

In the course of this paper, I will evaluate the possibility of introducing a right to de-list in Hong Kong as a means to enhance protection of citizens’ information that has been made publicly available. An understanding of privacy and personal data is essential for any issue related to privacy. Therefore, Part I seeks to elucidate the concepts of ‘privacy’ and ‘personal information’. I contend that a modern understanding of a right to privacy should take into account the context of the personal information and should incorporate a degree of protection for privacy in the public domain. In Part II, I discuss development concerning privacy rights and public data in English law and the jurisprudence of the European Court of Justice (“ECJ”) and the European Court of Human Rights (“ECtHR”). A focused

---


discussion of two recent important Hong Kong decisions, namely the Do No Evil App case and the David Webb case, will also be provided. From these, I identify features of expansion in protection of privacy rights in the English and EU jurisprudences, and I also explore the possibility of recognising a right to be forgotten in Hong Kong. This leads to my original argument in Part III—a proposal on introducing a narrow right to be forgotten into Hong Kong. I provide a workable approach that takes into account the local context and competing interests such as freedom of expression and public interests. In finding the delicate balance of competing interests, I consider the possibility of the newsworthiness defence amongst other exemptions and defences.

At the outset, a few clarifications are needed. The issue of leakage of personal data into the public domain is beyond the scope of this paper, and this is for an apparent reason: if the data is of a personal nature that should have never become public knowledge but for mistakes and accidents such as loss of USBs, this is usually an obvious case of violation of privacy of the victim and remedies should follow. Rather, this paper is chiefly concerned about the problem aroused from online intermediaries’ use of data that has already been publicly available. This issue is of a more controversial nature because it seems to be paradoxical to our common understanding shaped by philosophical and legal theories, which provide that privacy is of a private-public dichotomy nature and protection of privacy is focused on the private sphere. The issue discussed in this paper is hence worthwhile of a deeper discussion.

I. Understanding Privacy and Personal Information

‘Privacy’ has ‘come a long way’ since its original formulation by Warren and Brandeis as a ‘right to be let alone’. Since then, there have been various attempts to illuminate the concept of ‘privacy’. A lot of these attempts proceed from different values and perspectives, resulting in a discourse of privacy that is anything but consistent and coherent. A satisfactory definition of ‘privacy’ remains elusive. As conceded by Judith Decew, “It is not possible to give a unique, unitary definition of privacy that covers all the diverse privacy interests.”

---

6 R. Wacks, Privacy: A Very Short Introduction, Oxford University Press, 2010
While I share the sentiment that formulating a single definition of privacy is impossible because privacy issues involve a broad spectrum of matters including values, interests and power\(^8\), at the same time, I recognise it is equally unthinkable to leave the concept unexplained. A brief account is therefore provided below.

‘Privacy’, in its broadest sense, rests on an understanding of an individual and his/her relationship with the society. It is relational and norm sensitive. In formulating a concept of privacy, Westin conceives ‘privacy’ as a claim or a fortiori to determine when, how, and to what extent information about individuals is communicated to others\(^9\). However, Westin’s formulation of privacy as a claim fails to define the content of privacy\(^10\). A more acceptable description of ‘privacy’ should be in terms of the extent individuals can exercise their control over information about them in a specific context. The control-based conception better captures the autonomy aspect and values of privacy, and it reflects the choices one has over disclosing or keeping confidential of information about him/her. This understanding accords with traditional tort law that perceives privacy as an interest in ‘having control over information about oneself’\(^11\).

‘Privacy’ is also commonly understood as protection of ‘personal information’. But what is the meaning of ‘personal’? And under what circumstances is information considered to be ‘personal’?\(^12\) The difficulty here is that different people have different understanding of what is personal, sensitive and intimate. Information that I consider to be intimate and hence wish to withhold may not be considered to be so by others. Take for example the number plate of my car. It is hard to convince others that disclosure of my vehicle registration document is an invasion of my privacy of personal information.

However, a total subjective test of what is ‘personal’ is equally inconceivable, as it defeats the purpose of protection if virtually everything can be personal information as long as someone claims it is so. Therefore, there must be an objective criterion to determine what may legitimately be claimed to be ‘personal’. Any definition of ‘personal information’ should entail a commonly recognised quality of information that explains why an individual has reasonable expectations regarding its use and disclosure. A helpful explanation of ‘personal information’ is provided by Raymond Wacks: “[it] includes those facts, communications or opinions which relate to the individual and which it would be reasonable to

\(^10\) D.N. McCormick, “Privacy: A problem of Definition”, British journal of Law and Society 1, 1974, pg. 75
\(^11\) [Ibid 7]
\(^12\) These two questions are rephrased from that highlighted by Raymond Wacks in discussing the problem of privacy at the level of personal information. See Introduction of his book, *Volume I: The Concept of Privacy*, supra 5
expect him to regard as intimate or sensitive and therefore to want to withhold, or at least to restrict their collection, use or circulation”

A crucial matter in this paper is the assertion that we retain a degree of a right to privacy in relation to certain publicly available information. In other words, it involves the issue of privacy in the public domain. It was only until the recent two decades that discussion of our privacy rights in public started14. Philosophical and theories of privacy have long recognised a private-public dichotomy. The term ‘private’ is usually used to refer to the realm of familial and other personal relations, whereas ‘public’ indicates the realm of community outside the personal realm and may include government institutions15. A persistent normative understanding of these theories is that protection of privacy concentrates on the private sphere alone. It is henceforth suggested that these theories suffer from a ‘theoretical blind spot’ on the matter of privacy in the public domain16, and they do not reflect the new order shaped by technological advancement.

In the age of free flow of information facilitated by digitalisation, the private-public boundary is increasingly blurred. Data subject’s personal information is readily made publicly available through, for example, computerisation of public records by the government or the data subject’s previous intentional or unintentional disclosure. Privacy risk of these public data is even higher than data kept by persons in their private sphere because consent to use these public data is often seen to be unnecessary and unconceivable, as it is usually impossible for a third party that seeks to use the data to know the means to contact the person involved and ask for his/her permission. This sometimes leads to a mistaken view that if an individual willingly discloses information in the public sphere, he/she has ‘let the cat out of the bag’ and the now ‘public data’ can be used in any way by third parties. Traditional theories that assumes a clear boundary of what is public and private have to be re-examined in light of the new reality. As appropriately put forward by Helen Nissenbaum, a satisfactory understanding of a right to privacy must now incorporate a degree of protection of privacy in public17.

A further privacy issue that arises from information technology is that information can now be transferred easily from one context to another context, but what is not considered intimate in one context may be considered so in another context. For example, a person that is willing to have his medical history uploaded on the website of a medical school for educational purpose may not expect his medical record to be sent to his family or disclosed to marketing companies. ‘Privateness’ is not necessarily a feature or quality of the information itself. Rather, it is the context where the information is situated that

13 [Ibid 5], Introduction
14 The issue of privacy in public was first raised by Helen Nissenbaum in her article, “Protecting Privacy in an Information Age: The Problem of Privacy in Public”, Law and Philosophy, Volume 17, Issue 5, November 1998, pg. 559-596
16 [Ibid], pg.5
17 [Ibid 15]
determines its level of ‘privateness’ and the consequential extent of control one can exercise over such information. A modern conception of privacy has evolved from a ‘right to be let alone’ originally formulated by Warren and Bradeis to a new understanding of privacy as ‘contextual integrity’\(^\text{18}\). This understanding of privacy is in line with the norm-dependent and context-sensitive features of privacy.

Similarly, ‘publicness’ of information also varies with the different domains of the public sphere where the information is available. For example, before digitalisation of public records, one needs to travel to the place where the information is housed, such as the government office of the Companies Registry, to search for the paper records and make photocopies. The tediumness in accessing these records acts as a de facto protection of public data\(^\text{19}\). However, with computerisation and the emergence of online intermediaries, access to public records is made far more convenient and flexible. Consequentially, digitalised public data is exposed to a much more thoroughgoing sense of publicness than paper documents, even though both constitutes publicly available information.

II. Where Are Our Privacy Laws Heading To?

a. The English Law

Lord Hoffman in \textit{Wainwright v Home Office}\(^\text{20}\) drew a distinction between U.S. privacy law and the position of the English law and affirmed there is no general tort of invasion of privacy at common law. The same doubt on privacy rights is expressed in Hong Kong. Sir Derek Cons, V.P in \textit{Ex Parte Lee Kwok Hung}\(^\text{21}\) remarked, “I am not aware of any similar clearly defined or long established right with regard to privacy, which has always been a grey area of our law.”\(^\text{22}\)

The closest one could get to protect true information from embarrassing publicity is to invite the court to order equitable remedies for breach of confidence. Breach of confidence was once considered to be ‘the most effective protection of privacy in the whole of our existing civil and criminal law.’\(^\text{23}\) However, although there are overlapping between breach of confidence and privacy, breach of confidence, as I argue below, offers an inadequate protection of personal information. My submission that a remedy of


\(^{19}\) [Ibid]

\(^{20}\) \textit{Wainwright v Home Office} [2003] UKHL 53 (Lord Hoffmann said at [18], “The need in the United States to break down the concept of “invasion of privacy” into a number of loosely-linked torts must cast doubt upon the value of any high-level generalisation which can perform a useful function in enabling one to deduce the rule to be applied in a concrete case. English law has so far been unwilling, perhaps unable, to formulate any such high-level principle. There are a number of common law and statutory remedies of which it may be said that one at least of the underlying values they protect is a right of privacy.”)

\(^{21}\) \textit{Ex Parte Lee Kwok Hung} [1993] 2 HKLR 51

\(^{22}\) [Ibid], pg.63

\(^{23}\) \textit{Report of the Committee on Privacy} (Cmnd 5012, 1972) (Chairman: Kenneth Younger), 1972, para 87
breach of confidence is insufficient to safeguard privacy is shared by scholars such as Raymond Wacks\textsuperscript{24}, and recent judicial development also appears to support my view.

After the enactment of the Human Rights Act 1998 (which incorporates Article 8 of the European Convention of Human Rights into English law), it continues to extend a long arm into the English law, resulting in persistent evolvement in the action of breach of confidence. The court in \textit{Douglas v Hello! (No.3)} said that, “In order to find the rules of the English law of breach of confidence we now have to look in the jurisprudence of article 8 and 10 [of the ECHR]”\textsuperscript{25}. Over the course of development, especially in recent years, there has been a significant expansion for protection of privacy. The most notable development is the creation of a new tort of ‘misuse of private information’. In \textit{Campbell v MGN Ltd}\textsuperscript{26}, the House of Lords relaxed the traditional requirement of an \textit{a priori} existence of a duty of confidentiality and held that the duty could arise when a person obtains personal information the nature of which gives rise to a reasonable expectation of privacy \textsuperscript{27}. Lord Nicholls remarked that “the essence of the tort is better encapsulated now as ‘misuse of private information’.”\textsuperscript{28} Misuse of private information as a distinct tortious cause of action is confirmed in \textit{Google v Vidal-Hall}\textsuperscript{29}, where the court allowed a claim for misuse of private information where Google Inc’s has, without the claimants’ consent or knowledge, tracked and collated information relating to his Internet usage on the Internet browser. \textit{Google v Vidal-Hall} represents a further leap in the development of law in this area by establishing that browser-generated information may potentially constitute ‘personal data’.

While the development in the common law should be applauded for providing a better protection for personal and private information\textsuperscript{30}, it should be pointed out that neither \textit{Campbell} nor \textit{Vidal-Hall} has been applied in Hong Kong courts to recognise a distinct tort of ‘misuse of private information’\textsuperscript{31}. More importantly, despite an apparent effort to expand traditional doctrines to better safeguard privacy, inherent limitations of the breach of confidence remain.

\textsuperscript{25} \textit{Douglas v Hello! (No.3)} [2006] QB 125, para 11
\textsuperscript{26} \textit{Campbell v MGN} [2004] UKHL 22 (in which Ms. Naomi Campbell sued Mirror Group Newspapers for breach of confidence for publishing photographs of her leaving a Narcotics Anonymous meeting)
\textsuperscript{28} \textit{Campbell v MGN} [2004] UKHL 22, par 14
\textsuperscript{29} Judith Vidal-Hall & ors v Google Inc [2014] EWHC 13, 16 January 2014
\textsuperscript{30} In \textit{Sim Kon Fah v JBPB and Co. (A firm) & ors} [2011] 4 HKLRD 45, the court went even further and said the law on breach of confidence has substantially arrived at a position of protection from publicity of private information.
\textsuperscript{31} But the concept of “misuse of private information” has been considered in some recent cases. See \textit{X v Y} [2014] 5 HKLRD 823 (the plaintiff brought an action breach of confidence and/or misuse of private information, but the judge did not discuss if misuse of private information is a valid cause of action). See also \textit{Sim Kon Fah v JBPB & Co} [2011] 4 HKLRD 45 (the judge mentioned the concept of misuse of private information in discussing the development of the law of breach of confidence)
Primarily, to pursue the breach of confidence action, the claimant has to prove the confidential nature of the information. Following this, this action does not cover information that is available in the public domain, and it reveals its significant limitation in privacy claims in relation to the public domain. The court in *AG v Guardian Newspapers Ltd (No.2)*[^32] made it clear that once information has been publicly available, it loses its confidentiality nature. Recent cases also adopt a stringent attitude to public data. In *D v L*[^33], the court held that injunction will not be granted if the information is already in the public sphere. In another case, *Barclays Bank plc v Guardian News and Media Ltd*[^34], the court decided that the action does not protect information that is published on some ‘remote or expert website’, which the public cannot access without a great deal of effort. An action of breach of confidence therefore fails to recognise privacy problems in cases where personal data has been legitimately made publicly available but is subsequently misused by third parties. Privacy risk of personal data in the public domain has still not been taken seriously.

Furthermore, a relationship of confidence is essential for the action. But this may not be always present where the personal information of the claimant has been published without his/her consent by, for example, online blogs and newspapers, which collect the information legitimately and do not owe a duty of confidentiality to the claimant. Moreover, the application of the equitable maxim that the claimant must come with ‘clean hands’ becomes a barrier to a claimant who disclosed information on an earlier occasion, even though he did not intend the information to be used in another context.

b. The European Approach

For reasons of the limitations in the English law in relation to privacy protection identified above, I turn to the approach by the European Union to explore alternative means of safeguards for privacy. I however bear in mind that the European countries have a different legal system from Hong Kong, and cases of the ECtHR and ECJ are not binding on Hong Kong courts. The discussion below is meant to draw reference for a development direction of privacy law in Hong Kong.

The continental approach to privacy is formed on the basis of a ‘right of personality’[^35]. In addressing the categorization of privacy in Europe, Moreham draws a distinction between firstly, freedom from unwelcome active interference with individuals’ well-being or integrity and secondly, freedom to develop personality, autonomy, lifestyle, and identity[^36]. The conception of privacy as protection of the ‘dignity of man’ and the ‘right to develop personality’ is commonplace in constitutions or civil codes of European countries. For example, in Germany, the Basic Law provides that ‘Everyone shall have the

[^32]: AG v Guardian Newspapers Ltd (No.2) [1990] 1 AC 109
[^33]: D v L [2003] EWCA Civ 1169
[^34]: Barclays Bank plc v Guardian News and Media Ltd [2009] EWHC 591 (QB)
right to the free development of his personality in so far as he does not violate the rights of others or offend against the constitutional order or the moral code. Similarly, the Constitution of Italy sees a right to privacy as an element of an individual’s personality. The French Civil Code also provides that everyone should have the right to respect for his private life. The court has interpreted this statute as including protection for information relating to a person’s identity (such as name, date of birth, address, etc) and other personal information such as matrimonial status, health, sexual orientation and his/her way of life in general.

The introduction of the European Convention of Human Rights has escalated a right to privacy as a well-recognised human right. The current legal framework of personal data protection is encapsulated in the Data Protection Directive 95/46/EC (“1995 Directive”) and the Directive on privacy and electronic communications 2002/58/EC. Under the EU law, there are strict conditions for legitimate gathering of personal information. Persons or entities that collect and manage personal data must protect it from misuse and must respect certain rights of data owners safeguarded under EU law. More specifically, under Article 12 of the 1995 Directive on right of access, it provides that a person can ask for his personal information to be deleted once that data is no longer necessary.

The ECtHR and ECJ have been active in clarifying and reshaping data privacy law in the continental jurisdiction. I will highlight several key cases that deal with the problem of privacy of public data and what Hong Kong can learn from them.

The first of them is the well-known Google Spain case. The applicant is a Spanish national resident. He lodged a complaint against Google Spain and Google Inc. on the fact that when an Internet user entered his name in Google Search, he would obtain links to two pages of newspapers in 1998, in which an announcement mentioning his name appeared for a real-estate auction connected with attachment proceedings for the recovery of social security debts. In deciding the case, the ECJ held that the 1995 Directive is applicable to search engines. Article 12 provides that individuals have a right to request data controllers to remove links to third party webpages when the information is ‘inaccurate’, ‘inadequate’, ‘irrelevant’, ‘no longer relevant’, or ‘excessive for the purposes of the data processing’ under Article 6. Crucially, the ECJ confirmed that search engine operators qualify as ‘data controllers’ pursuant to Article 2(d) on the basis that the search engine operator determines the purposes and means of data processing, and therefore search engines are subject to the 1995 Directive.

To better protect our privacy rights from interference of online intermediaries, I submit that a similar position should be adopted in Hong Kong, so that online intermediaries such as search engines and

---

37 Article 2(1) of the Constitution of Germany
38 Article 9 of the French Civil Code
40 Google Spain, para 14
websites would, similarly, be qualified as ‘data users’ (the equivalent of ‘data controllers’ in the 1995 Directive\textsuperscript{41}) pursuant to the Personal Data (Privacy) Ordinance (“PDPO”) and would hence be subjected to regulation. I will discuss the proper ambit of ‘data users’ in Part III when I explain my proposal for reform of privacy laws in Hong Kong.

The second case is the Satamedia case. This case is brought to special attention as it shares similar factual background with the Do No Evil App case in Hong Kong. The Satamedia case concerns publication of taxation data about natural persons. The taxation information is a public record in Finland and is publicly available. Satamedia collected records of 1.2 million people from the public domain and published them on its magazine. Although these public records have always been made publicly available by the government and Satamedia did not acquire the data by illicit means, the ECtHR nonetheless held that Satamedia has intruded the data protection law. In considering the defence of journalistic activities, the ECtHR agreed with the finding of the Finnish Supreme Administrative Court “that the publication of the whole database collected for journalistic purposes could not be regarded as journalistic activity” and that the public interest did not require such an extent of publication of personal data\textsuperscript{42}. It is argued that the ECtHR’s approach in Satamedia should have been considered in the then Privacy Commissioner’s report on the Do No Evil App case, which will be explained below.

The third one is the Client Earth case\textsuperscript{43}. It is an ECJ decision after the Google Spain case. The applicant requested access to several documents concerning the EFSA’s draft guidance. EFSA granted the individual comments of the external experts but redacted their names. The names of these experts, together with their opinions on the draft guidance, were however published on the website of EFSA. The case is highlighted as it affirms the position that publicly available information may not necessarily be characterised as personal data. Similarly, information submitted for the purpose of a professional activity does not alter the nature of information as personal data. The ECJ emphasised that the concepts of ‘personal data’ and ‘data relating to private life’ should not be confused\textsuperscript{44}. A claim that the information in question does not fall within the scope of the private life of the experts must therefore be regarded as unacceptable. The ECJ has shown a proper attitude to publicly available information, which, I submit, should be adopted in Hong Kong. In fact, the then Privacy Commissioner also shared the same sentiment. In his report on the Do No Evil App case, he said, “This case underlies a myth

\textsuperscript{41} Hogan Lovells, “A Right to be Forgotten in Hong Kong?”, 2015, \url{http://www.hoganlovells.com/files/Uploads/Documents/Newsflash_A_Right_to_be_Forgotten_in_Hong_Kong_HKGLIB01_1452118.pdf} (accessed on 20 October 2015)

\textsuperscript{42} Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland 931/13 - Chamber Judgment [2015] ECHR 713 (21 July 2015), para 70.

\textsuperscript{43} Client Earth et al. v. EFSA, JUDGMENT OF THE COURT (Second Chamber) (16 July 2015), \url{http://curia.europa.eu/juris/liste.jsf;jsessionid=D9ea7d0f130d59ef200135aed4fbea63f81d966b05bea.e34KaxilC3eQc40LaxqMbN4OchaNe0?num=C-615/13&language=en} (accessed on 10 January 2016)

\textsuperscript{44} [Ibid], para 32.
commonly held by people, namely personal data collected in the public domain, not from the data subjects direct, is open to unrestricted use. This is incorrect.”

On 15 December 2015, the European Parliament, the Council and the Commission reached an agreement on European Commission’s EU data protection reform. The new rules aim at enhancing existing rights of EU citizens and empowering them with greater control over their personal information. One of the main focuses of the reform is to strengthen the ‘right to be forgotten’ in an online environment. The proposed regulations clarify and affirm a ‘right to be forgotten’; Article 17 is specifically dedicated to ‘the right to be forgotten and to erasure’. Essentially, it says, when an individual no longer wants his/her data to be processed, he/she can request for deletion of the data, provided that there are no legitimate grounds for retaining it. It is believed that codification of a ‘right to be forgotten and erasure’ in the reform of EU data protection regulations will further enhance European citizens’ fundamental privacy rights in the information age, particularly their ability to erase information about them in the public domain.

c. Reflections from the Do No Evil App and the David Webb cases in Hong Kong

*The Do No Evil App case*

The Smartphone Application “Do No Evil App” (“the App”) includes a database of public information such as litigation, bankruptcy and company directorship data. The App allows a user to search for records of an individual, including his/her name, personal identity card number, address, court type and action number (if the individual has been in a criminal, civil or bankruptcy cases), company directors’ data and more. The then Privacy Commissioner decided that the App’s use of complainants’ litigation, bankruptcy, etc data for due diligence has exceeded the complainants’ “reasonable expectation” as to how such information in the public domain would be used. Their use of data is not consistent with or directly related to the purposes of collection and publication by governmental institutions such as the Judiciary, the Official Receivers’ Office and the Company Registry. Consequentially, the data operator has contravened Data Principle 3 (“DPP3”), which concerns the purpose of usage of data at the time of collection.

The operation of ‘Do No Evil App’ is similar to Satamedia in the sense that they both involve usage and publication of data that is already in the public domain. The two decisions share the assumptions that certain public records may be personal in nature, and despite being available in the public domain, these public data shall be used only for a limited purpose. However, the bases of decision are slightly

---

45 Office of the Privacy Commissioner for Personal Data, Hong Kong, “Report Published under Section 48(2) of the Personal Data (Privacy) Ordinance (Cap.486)”, 2013, para 75.
46 European Commission, “Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general Data Protection Regulation)”, pg. 25
47 [Ibid 45]
different. *Do No Evil case* focuses on the use of data by intermediaries that is inconsistent with the *purpose* of original publication in the public domain, whereas *Satamedia* case held that there is a violation of right to private life as the *extent* of publication of 1.2 million people’s taxation information on a magazine is beyond the scope of defence of journalistic activities.

Anyway, as the two cases’ factual background are similar, the then Privacy Commissioner should have referred to the *Satamedia* case and other relevant case authorities in his investigation report. The then Privacy Commissioners’ decision is restricted to the interpretation of DPP3. Discussion of overseas authorities would not only provide further support to his decision, but it would also bring in discussions of applying a broader approach to privacy rights that has been accepted by the international community in Hong Kong.

*The David Webb case*48

Mr. David Webb is the founder and operator of Webb-site.com (“the Webb-site”). The Webb-site provides a “people-search” function that allows users to look for information of target persons. Information revealed includes directors of Hong Kong listed companies, members of public statutory and advisory boards, and licensees under the licensing regime of the securities and Futures Commission, etc. The personal data at issue are the full names of the complainant set out in the judgments of a matrimonial case heard in open court in Hong Kong. The complainant discovered that by using her name as search term, the Webb-site revealed hyperlinks connecting to the three anonymised judgments in the LRS. She asked Mr. Webb to delete the hyperlinks but her request was declined. She then lodged a complaint with the Privacy Commissioner. The Privacy Commissioner conducted an investigation and issued an enforcement notice on 26 August 2014 directing Mr. Webb to delete the hyperlinks at issue. Mr. Webb lodged an appeal against the enforcement notice on 11 September 2014 to the AAB. The appeal was dismissed.

Before the decision by the Administrative Appeals Board (“the AAB”) on the *David Webb case* was released, I had hoped that the case would establish a step closer to recognising a “right to be forgotten” in Hong Kong as the then Privacy Commissioner, Mr. Allan Chiang, had openly urged Google Inc to extend the “right to be forgotten” to Hong Kong and non-EU countries after Google Inc created ‘right to be forgotten’ forms for EU citizens in light of the *Google Spain* ruling. However, to my slight disappointment, the AAB adopts the same restrictive approach as in the *Do No Evil App* case by constructing the matter squarely as a violation of DPP3, without discussing the English or EU approach on similar issues.

---

48 Administrative Appeals Board, Administrative Appeal No. 54/2014 *David M Webb v Privacy Commissioner for Personal Data* (ABB 54/2014)
Dismissing Mr Webb’s appeal, the AAB concluded that Mr. Webb has contravened DPP3 of the PDPO. It held that DPP3 is directed against misuse of personal data regardless of whether the relevant personal data has been published elsewhere or is in the public domain. On a proper construction of subsection 4 of DPP3, the phrase ‘the purpose for which the data was to be used at the time of collection of the data’ refers to the purpose for which the data was originally collected. The gist of the AAB’s decision is that Mr. Webb was regarded as a ‘data user’ pursuant to the PDPO, and he had contravened DPP3 of the PDPO by using the complainant’s personal data for a “new purpose” inconsistent with the purpose of original publication in the public domain without express and voluntary consent by the data subject.

It is true that the David Webb case is not completely comparable with the Google Spain case because, as pointed out by the new Privacy Commissioner, Mr. Stephen Wong, while in the David Webb case the data subject’s name in her judgments has been redacted upon her request, there is no redaction of the newspapers articles in concern in the Google Spain case. Also, the basis of action in the two cases are different. The David Webb case turned on a finding that the data has been used for a new, inconsistent and unrelated purpose from which it was originally collected. The ruling was however different in the Google Spain case. The ECJ held that Google Inc had breached Article 6(1)(c) of the Directive because in the course of time, the data in question had become incompatible with the Directive in the sense that it was no longer adequate, relevant and not excessive in relation to the purposes for which it was collected.

Nevertheless, the Do No Evil App and David Webb cases are worth noting for a few points. For one, they affirmed the clarification by the then Privacy Commissioner that personal data collected from the public domain is not open to unrestricted use. For another, they confirmed that a data user would be liable when it, without the data subject’s prescribed consent, uses personal data for a new purpose or a purpose which is inconsistent with the original purpose of data collection within the meaning of DPP3 of the PDPO. Moreover, both cases established that an online intermediary that enables search for target individuals’ information published in the public domain could qualify as a ‘data user’ and hence be held liable under the PDPO. The David Webb case takes a step further than the Do No Evil App case as it effectively enforces a private individual’s request to order a database operator to remove hyperlinks from its website.

49 [Ibid 48], para 36. The AAB quoted the judgment by Chu JA at para 52 of Re Hui Kee Chun (with whom Yeung VP and A To J agreed), “It is irrelevant that the name, employment and job title of Mr. Tam could be ascertained from other sources or had been carried in the newspapers reports or were otherwise publicly available. DPP3 prohibits the use of personal data without the consent of the data subject for a purpose different from the original collection purpose or directly related purpose. It is directed against the misuse of personal data and it matters not that the personal data involved has been published elsewhere or is public available. This is entirely consistent with the objective of the PDPO to protect personal data”.

50 [Ibid 48]

The *David Webb* case appears to recognise a certain form of *right to de-list* enforceable by a private individual, although this is not expressly spelled out in the decision, which is perhaps a deliberation by the AAB not to touch on the controversial right to be forgotten.

As the decisions stand now, there clearly is some basis in Hong Kong law, or at least in the enforcement policies of the Privacy Commissioner, for a narrow right to be forgotten, such that a database operator could be compelled to remove hyperlinks connecting users to the data subject’s personal data in the public domain. However, still, we should bear in mind that the judicially sanctioned “right to be forgotten” in the *Google Spain* case is a narrow one and should more appropriately be named as a “right to de-list”. According to the ECJ ruling, search engine operators are obliged to remove hyperlinks from (i.e. de-list) Internet search results. The content of the third party webpages remains intact and can be accessed by searching with search terms other than the individual’s name.

### III. Implementing a Right to De-list in Hong Kong

#### a. Why it is important to discuss the possibility of introducing a right to de-list in Hong Kong

With the perhaps deliberate avoidance to discuss a right to be forgotten or a right to de-list, the then Privacy Commissioner and the AAB have missed the opportunity to clarify the position in Hong Kong in view of the international development of privacy laws. This leaves many unanswered questions in the air: for example, following the *David Webb* and *Do No Evil* cases, is it now a general position in Hong Kong that personal data lawfully available in the public domain cannot be collected to form an online database enabling a search of information about people listed in these public documents? Can an individual enforce his right to request intermediaries to remove search results connecting to public domains directly against the intermediary? Or must he do so through lodging a complaint with the Privacy Commissioner?

The purpose of Part III aims at eliciting discussion from a legal perspective of whether Hong Kong citizens should have control over personal information in the public domain. It is important to clear the air after the *David Webb* case, and also to address uncertainties concerning Hong Kong’s position in view of a more receptive attitude to expansive approach in privacy protection found in late English and continental jurisprudence. The time has now come to consider the possibilities of implementing a right to de-list in Hong Kong.
b. Understanding privacy as a right to control

As Judith Decew remarked, “autonomy is required for people to express themselves”\(^{52}\). Autonomy is understood as control that one has over his/her private life and values. In the words of John Stuart Mill, privacy allows us to be free from overreaching social influence\(^ {53}\). But privacy is more than giving us the essential control to restrict others’ access and intrusion into our personal information in private lives. It also covers protection of information in all other domains and contexts\(^ {54}\). On this basis, Judith Decew offered three categories of privacy: informational privacy, accessibility privacy, and expressive privacy\(^{55}\). The advantage of understanding privacy as an ‘expressive privacy’ is that it recognizes self-expression and the ability to form interpersonal relationship. This, in my opinion, better captures the importance of a right to control over personal data—as a form of expression of self-identity and regulation of self-control.

Furthermore, a control-based understanding of privacy reflects the relational dimensions of privacy. It draws the boundary of personal and intimate information from non-personal and insensitive information and features the distinctive extent of control in these different social situations. This would encourage a greater respect to one another’s private sphere as well as facilitate deeper social relationship with others. Also, determination of the extent of control varies in different contexts and is norm-sensitive, as mentioned in Part I. My view is supported by philosophical and legal arguments that social norms shape an individual’s understanding of his/her relationship with the society, such as Schoeman’s theory of social norms as a function to protect human dignity\(^ {56}\). Most notably, the requirement of an element of control in a right to privacy is reflected from the definition of ‘data user’ in section 2 of the PDPO, which defines a ‘data user’ as a person\(^ {57}\) who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data\(^ {58}\).

c. The Proposal

A newly codified right to de-list would enable an individual to, *inter alia*, compel online intermediaries to take the content down if it connects to personal data in the public domain or prohibit further use of it where appropriate. This would accord greater protection of the right to privacy and right to self-
determination of Hong Kong citizens. More importantly, this would provide certainty in our privacy laws and further affirm the position from previous Hong Kong cases that public data of individuals is subject to data regulations, and a proper understanding of privacy must contain an element of control over our public data. As opposed to a broadly worded right to erasure under the EU data protection regime, a right to de-list would not result in deletion of information from original sources and would, as illustrated below, be compatible with Hong Kong constitutional rights such as freedom of expression.

It is hoped that the new Privacy Commissioner would take a more earnest and open attitude to protection of privacy of public data in Hong Kong and consider my proposal below.

i. Reframing statutory definition of data user

There has been constant litigation concerning the definition of ‘data controller’ in Article 2(d) of the 1995 Directive (an equivalent of “data user” in the PDPO59). In particular, there is an inconsistent perception of intermediaries such as search engines in the body of English and European case law as to whether they are ‘mere conduit’ or ‘passive facilitator’ as opposed to intermediaries that ‘facilitate access to websites provided by others’60.

In view of the seriousness of potential harm caused by disclosure of highly sensitive information, features of automatic generation of data operators should not be an excuse for intermediaries to escape from liability over information on their platforms. My sentiment is resonated by a recent Court of Final Appeal decision, which seems to settle the position in Hong Kong in relation to the role of search engines, at least for now. In Dr. Yeung Sau Shing61, a defamation case, the defendant, Google Inc, contended that the autocomplete and related searches functions of Google Inc are neutral tools. This is rejected by the Court of Final Appeal. The Court observed that Google search’s algorithms and its autocomplete feature “act by providing information distilled pursuant to artificial intelligence set up by Google Inc themselves by virtue of the algorithms they have created and maintained to actively facilitate the search processes”62.

Although Yeung is a defamation case, it shows the Hong Kong court’s willingness to hold intermediaries liable for information posted on their platforms. Similarly, in Google v Vidal-hall63, the English Court

59 [Ibid. 41]
60 See Byrne v Deane [1937] 1 KB 818, Trkulja v Google Inc LLC (No 5) [2012] VSC 533, A v Google New Zealand Ltd [2012] NZHC 2352, Oriental Press Group Ltd v Fevaworks Solutions Ltd (2013) 16 HKCFAR 366, Tamiz v Google Inc [2013] EMLR 14, and Bleyer v Google Inc [2014] NSWSC 897. These cases are inconsistent and contradictory. For example, McCallum J in Bleyer declined to apply Trkulja and chose to follow the English authorities and held that Google Inc could not be liable as a publisher of results produced by its search engine, and hence innocent dissemination was inapplicable. Whereas in Fevaworks Solutions Ltd, the Court of Final Appeal has expressly parted ways with Tamiz and rejected the conflation of the innocent dissemination defence. It should be noted that Dr. Yeung Sau Shing applied Fevaworks on the issue of the role of search engine.
61 Dr. Yeung Sau Shing Albert v Google Inc [2014] 4 HKLRD 493
62 [Ibid], para 116
63 [Ibid. 29]
confirmed that misuse of private information is a distinct tortious cause of action applicable to search engines, and more importantly, it held that browser-generated information may potentially constitute ‘personal data’.

The role and scope of liability of online intermediaries should be clarified in PDPO to avoid inconsistencies as currently found in contradicting EU and common law jurisdictions. Accordingly, the definition of ‘data user’ in section 2 of PDPO should be amended. It should explicitly list out criteria that will qualify online intermediaries to become ‘data users’ which are then subject to privacy regulations in Hong Kong. Also, the position of search engines should be explained in the statute for consistency of court application in the future.

ii. The three criteria approach

It is proposed that a right to de-list should be applicable to online intermediaries in Hong Kong that i) have knowledge of their hosting of third-party content (i.e. the knowledge criterion), ii) have a realistic ability to control publication of content (i.e. the control criterion), and iii) compile information about an identified person or about a person whom the data user intends or seeks to identify (i.e. the compile criterion). This proposal partially adopts the test in defamation formulated by Ribeiro PJ in the Fevaworks case. Although the nature of a defamation action and a privacy claim is different, recent development in Hong Kong and English jurisprudence shows that the boundary between the two is a ‘fuzzy’ and blurry one. Because of their similarities and overlapping, insights from defamatory principles which are built on solid foundation in age-old precedents, among other things, could form a feasible framework for reference in implementing a new right of a right to de-list.

Knowledge criterion: ‘knowledge’ is taken to mean ‘a degree of awareness or at least an assumption of general responsibility’ as identified by Eady J in Bunt v Tilley. Agreeing with Eady J’s observations, Ribeiro PJ in Fevaworks said the knowledge criterion “should be taken to mean that the publisher must know or be taken to know the content —not necessarily every single word posted—but the gist or substantive content of what is being published”; it is “irrelevant whether the provider realised that such content was in law defamatory”. There is no reason why the same observations should not apply to online intermediaries in relation to privacy rights. In the context of privacy and particularly in relation to a right to de-list, an online intermediary should be deemed to have acquired knowledge of the content

---

65 R. Wacks, Privacy and Media Freedom, Oxford University Press, 2013, pg. 180-181
66 Bunt v Tilley [2007] 1 WLR 1243
67 [Ibid. 64], para 84
68 [Ibid. 64], para 84. For a more in-depth analysis of the relationships among defamation, Internet intermediaries, publication and the innocent dissemination defence, please see Mr Justice Ribeiro’s speech at the Hong Kong Judicial Colloquium 2015. http://www.hkcfa.hk/filemanager/speech/en/upload/139/Defamation%20and%20Internet%20Intermediaries.pdf (Accessed on 29 June 2016)
infringing person data if they are, for example, notified by a data subject or the Privacy Commissioner through a complaint or removal request. As shown, knowledge and control of intermediaries are intertwined. The question of control was discussed in Google Spain, in which the ECJ rejected Google’s argument that it has no knowledge of the data in concern and does not exercise control over the data, and found the operator of the search engine is regarded as a ‘data controller’. But note that under my formulation, knowledge of content would not mean that the intermediaries’ liability automatically ensues, even if the information turns out to infringe data privacy of the data subject. It is because to hold it otherwise will be too burdensome for intermediaries. The knowledge criterion has to be read with an approach requiring ‘reasonable efforts’, which will be explained below.

Control criterion: requirement of a control element is in fact inclusive in the definition of ‘data user’ in section 2 of the PDPO. It defines a ‘data user’ as a person who, ‘either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data’. Internet discussion forum, blogs and Apps would have the essential control element and hence normally fall under the head of ‘data user’ as they comprise a closed group of users who agree to abide by the rules (eg. Service Agreement when downloading the App) and the owners have the capacity and responsibility for editorial control over content. Furthermore, the position of search engines and online database platforms must now be viewed in light of the Yeung case. It is certainly a potential argument that these online intermediaries serve more than a ‘mere conduit’ and consequently exercise control over personal data that they collected from the public domain and publish on their platforms.

Compile criterion: element of compilation of information is essential in deciding whether an intermediary is handling data in a way that would subject itself to privacy regulations. In the landmark case of Eastweek, Ribeiro JA (as he then was) pointed out that “It is… of the essence of the required act of personal data collection that the data user must thereby be compiling information about an identified person or about a person whom the data user intends or seeks to identify.” The statement lays down two conditions for an act to qualify as collection of personal data: a) the collecting party must be thereby compiling information about an individual; and b) the individual must be one whom the collector of information has identified or intends or seeks to identify.

---

69 The Office of the Privacy Commissioner for Personal Data stresses that the definition of “data user” is not confined to institutions alone but it also covers any individual that “controls the collection, holding, processing or use” of personal data. See Data Protection Principles in the Personal Data (Privacy) Ordinance– from the Privacy Commissioner’s perspective (2nd Edition), Chapter 4. In relation to the government, the word “person” is defined in section 3 of the Interpretation and General Clauses Ordinance (Cap. 1) to include “any public body and any body of persons, corporate or unincorporate, and this definition shall apply notwithstanding that the word ‘person’ occurs in a provision creating or relating to an offence or for the recovery of any fine or compensation.”

70 The PDPO, section 2

71 Eastweek Publisher Limited & Another v Privacy Commissioner for Personal Data [2000] 2 HKLRD 83
iii. Reasonable efforts

Under the current legal framework in Hong Kong, the press is allowed to get away from liability of publication of information if it is considered as a journalistic activity and the data user in the press reasonably believes that the publication is a matter of public interest. As recognised in landmark case authorities such as Jameel\(^72\) and Grant v Torstar Corp\(^73\), traditional media such as newspapers can avail themselves of a public interest defence, or alternately called the responsible communication defence, insofar as they reasonably or responsibly believe that the publication furthers the public interest. As Lord Hoffman made it clear in Jameel, the question in each case is whether the defendant behaved fairly and responsibly in gathering and publishing the information. It is submitted that the same liberal approach should be conferred to online intermediaries, which, as identified by Dr. Marcelo Thompson, are faced with greater challenges on the condition of their responsibility\(^74\).

Although I draw reference to the defamatory law partially in formulating a three-criteria approach to a right to de-list above, I should note that the ‘reasonable efforts’ limb of my proposed right to de-list is distinct from the strict liability approach in defamation law\(^75\). The position of the current defamation law is that liability could accrue simply from knowledge of the content that turns out to be defamatory: once an intermediary knows or ought reasonably to be aware of the content of the article complained of, though not necessarily of its defamatory nature as a matter of law and has a realistic ability to control publication of such content, it would be obliged to take all reasonable steps to remove the offending publication\(^76\). Mere failure to take the content down would render intermediaries responsible for the damage of the defamatory content and impossible to avail themselves of a defence of innocent dissemination.

The strict liability approach found in defamation law is inapplicable for privacy claims concerning online intermediaries, because otherwise, the responsibility on online intermediaries in reaching decisions will be extremely huge. We should not expect perfection from intermediaries given their special nature as conduits of information collected from the public domain, which makes them different from original publishers.

It is therefore submitted that a reasonable and responsible publication approach should be applicable to online intermediaries. The normative dimension of intermediary responsibility requires intermediaries to devote ‘reasonable efforts’ in the circumstances to ascertain the nature of the content and exercise reasonable care to the thought processes by which they choose their reasons for action\(^77\). This also

\(^72\) Jameel (mohammed) v Wall Street Journal Europe Sprl (No 3) [2007] 1 AC 359
\(^73\) Grant v Torstar Corp 2009 SCC 61
\(^74\) M. Thompson, Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries, 2015, pg.50-56
\(^75\) Godfrey v Demon Internet Ltd (Application to Strike Out) [2001] QB 201
\(^76\) Dr. Yeung Sau Shing, the judge referring to the ratio by Ribeiro PJ in Feavaworks Solutions Ltd
\(^77\) [Ibid 74]
accords with the growing acceptance in common law jurisdictions of the concept of ‘reasonable expectation of privacy’\(^{78}\). What is reasonable depends on the context and facts of individual cases. The ‘reasonable effort’ approach takes into account a wide range of factors such as practicality, economic reality and technological means. Notification from data subjects or other bodies such as the Privacy Commissioner would be a relevant factor in considering what corresponding reasonable decision an online intermediary should make. By according a margin of appreciation to intermediaries, this approach can achieve the proper balance between on one hand, enhancing data subject’s control the use of their data by intermediaries, and on the other hand allowing greater flexibility to online intermediaries that accords with the reality. For example, when online intermediaries have actual knowledge of the third-party content they host and receives complaints from individuals alleging a violation of their privacy, the online intermediaries should reasonably ascertain whether the display of the content has contravened DPP3 and other privacy laws. The hosting of third-party content would be illegal when the purpose is inconsistent with the original purpose of collection of data in the public domain, or if it is a new purpose within the meaning of DPP3 of the PDPO.

An expectation of ‘reasonable efforts’ reflects a modern understanding of Internet intermediaries, which “must be seen not as mere keepers of gates but as designers of artefacts whose use plans settle normative questions and play a fundamental role in the construction of our normative reality”\(^{79}\).

iv. Balance between a right to de-list and freedom of expression

An inescapable controversy to any claim of privacy is how privacy rights can be balanced against competing interests such as free speech. However, finding the right balance is not easy. One of the reasons, as acknowledged by Raymond Wacks, is that the social function of ‘privacy’ makes the task of differentiating privacy from those of freedom of expression more difficult\(^{80}\). There is also an issue of public interests. Media such as the newspapers will argue that, for example, a celebrity’s birthday information available at Birth Registries in Hong Kong is a public interest and the public has a right to know, even though the celebrity wishes to conceal her age. A right to de-list is even more problematic than a common issue of privacy as it seems to be counterintuitive to people influenced by the old

\(^{78}\) Reasonable expectation of privacy is a well-established right in English law, see *Imerman v Tchenguiz* [2011] 2 WLR 592 and *Campbell v MGN Ltd* [2004] 2 AC 457. Although the concept of ‘reasonable expectation of privacy’ is not found in the PDPO or the Basic Law, it has in fact been well accepted by Hong Kong courts. For example, the *Imerman* and *Campbell* cases were applied and considered respectively in *Sim Kon Fah v JBPB and Co. (A firm) & ors* [2011] 4 HKL RD 45. The Court of First Instance affirmed that a claimant’s reasonable expectation of privacy could not be deprived of by the mere fact that the documents in concern were stored in a computer whose owner is entitled to search it for documents. See also *Keen Lloyd Holdings Ltd v Commissioner of Customs and Excise and another* HCAL 113/2012, 82/2013. More notably, in the *Do No Evil App* official report (*supra* 45), the then Privacy Commissioner stated that the App’s aggregation of personal data had exceeded the reasonable expectations of individuals of the use of their data.

\(^{79}\) [*Ibid* 74], Abstract

understanding of privacy that draws a rigid private-public distinction, and these people therefore may not appreciate the importance of protection of privacy in public domain.

Freedom of speech, the press and of publication are guaranteed under Article 27 of the Hong Kong Basic Law. Moreover, Article 19(2) of the International Covenant on Civil and Political Rights (which is incorporated into the Basic Law through Article 39) affirms a right to freely express our opinions without interference. However, it is not an absolute right and is subject to certain restrictions. Article 16 of the Bill of Rights Ordinance provides that any restriction on free speech must be ‘provided by law’ and are ‘necessary’.

Broadly speaking, justifications for freedom of expression is founded upon a consequentialist or a right-based approach. John Stuart Mill, a notable consequentialist scholar, laid down the foundation of free speech based on his argument from truth. But a problem with his formulation is that it would prevent any limitation on the exercise of a right to expression as long as the statement is true. Rights-based arguments are more desirable as they reflect that a right to privacy facilitates protection of personal autonomy. I am therefore more inclined to Alan Westin’s formulation of privacy as a means to enable us to be free from manipulation of others and allows us to release our emotions, as well as an ability to exercise control over our personal data depending on different contexts.

It is submitted that a right to de-list can be reconciled with the freedom of expression. This is achieved by a case-by-case assessment of the circumstances of a case and the type of ‘personal information’ involved. It is context-specific and is sensitive to public interest of accessibility to information. In ascertaining whether an online intermediary should be held liable, the court should conduct a balancing exercise. This involves taking into consideration different interests and according a margin of appreciation to intermediaries by considering, for example, their different extent of financial and technological capacities. My proposal could strike a proper balance between a right to de-list and freedom of speech, the press and publication, particularly so when it is open for the defendants to raise the defence of responsible communication or alike. As such, a recognition of a right to de-list is unlikely to bring chilling effects on the media.

v. Defences and exemptions

As mentioned, the right of privacy of individuals is not absolute. It must be balanced with other rights such as freedom of press and public interests. Therefore, defences and exemptions to a right to de-list should be available. This section explores different models of defences and exemptions in different jurisprudences in order to draw insight into formulating a workable right to de-list in Hong Kong.

*The Singaporean public domain defence*

---

82 See further in Part I
In Singapore, Personal Data Protection Act 2012 lays out the foundation of a public domain defence—organisations could collect, use and disclose publicly available personal data without the individual’s consent. This defence provides for an exemption of facts that can be found in records that are readily accessible to the public, or have come into the public domain through no fault of the defendant. However, it is noted that there is no blanket public domain exemption in other common law jurisdictions except Singapore. A further point to add is that the Law Reform Commission of Hong Kong has expressly rejected a public domain defence and considered it unnecessary and inappropriate. They observed that the absence of a public domain defence would not impinge on press freedom, but availability of this defence would encroach on privacy rights of individuals. I agree with the Law Reform Commission.

Imagine, if Hong Kong law allows for a public domain defence, a victim of unwarranted publicity would be unable to seek redress, for example, from persons that had given publicity to his private details in the public domain, even if the publicity amounts to a serious and unjustifiable infringement of his privacy. A public domain exemption approach should not be adopted in Hong Kong.

**Strict liability**

Strict liability is also inconceivable. A strict-liability regime threatens freedom of expression. It is opposed to another extreme end of no-liability regimes, which jeopardise individuals’, *inter alia*, privacy, reputation and racial integrity. A common ground between strict liability and a complete exemption of public domain should therefore be steered.

**Defence of journalistic activities**

Part VIII of the PDPO specifically covers a wide range of exemptions from the application of DPP3, and the then Privacy Commissioner has confirmed that they apply equally to personal data in the public domain. One of the key exemptions in relation to privacy in public domain is the news activity exemption provided for in section 61 of the PDPO. It states that personal data is exempt from the protection of DPP3 under two conditions: i) the data user’s whole or part of business consists of a news activity and the personal data is used solely for the purpose of that activity or any directly related activity; and ii) such disclosure is made by a person who has reasonable grounds to believe, and reasonably believes, that the publishing of the data is in the public interest.

---

83 Personal Data Protection Act 2012 (No. 26 of 2012), section 17 and Schedules 2, 3 and 4
86 [Ibid], para 60-63
However, the exemption is a narrow one as journalistic activity must relate to news or current affairs as provided in subsection 3. This makes the statutory news activity exemption much narrower than the defence of journalistic activities in the EU jurisprudence.

As highlighted by the ECtHR in the Satamedia case, activities may be classified as ‘journalistic’ under Article 9 of the EU 1995 Data Protection Directive if their sole object is the disclosure to the public of information, opinions or ideas, irrespective of the medium used to transmit them. This brings the defence of journalistic activities much wider than that provided for in the PDPO. The objective of Article 9 in the Directive is to reconcile competing interests of privacy rights and freedom of expression. This requires member states to provide exemptions or derogations in relation to personal data if the processing of data is carried solely for journalistic purposes or the purpose of artistic or literary expression. The court confirmed that a broad interpretation of notions of freedom, such as journalism, is as necessary as ensuring a freedom of expression in every democratic society. Hong Kong laws should therefore keep up with the evolvement in journalistic activities where there are new forms of media other than traditional news media and should develop a workable defence in face of the new reality.

Public interest defence

There is a limited public interest defence in the English law. For example, in Goodwin v United Kingdom88, a case concerning whether a journalist is required to disclose his sources, it was held that protection of journalistic sources is one of the basic foundations in a democratic society, and any measure requiring disclosure must be justified by an overriding public interest and freedom of expression that is prescribed by law and is pursuant and proportional to a legitimate aim89. However, Hong Kong courts appear to be reluctant to recognise a judicial public interest defence90 although a defence of public interest is set out in in section 61 and 64 of the PDPO (which covers offences for disclosing personal data obtained without consent from data users).

But the so-called public interest defence in these sections are unsatisfactory, primarily because the term ‘public interest’ is not defined in the statute and this may give arise to potential uncertainty. Therefore, one has to turn to other sources to understand the term. A helpful test of public interests is provided by Raymond Wacks in his book Protection of Privacy. It takes into account a wide range of factors such as whether the claimant consents to publication and whether the claimant is a public figure. As explained by the ECJ in the Google Spain case, the balance between protection of interests of internet users and others’ rights and freedom should reflect the ‘personal’ nature of the information in concern and the

---

88 Goodwin v United Kindgdom (1996) 22 EHRR 123
89 Ashworth Hospital Authority v MGN Ltd [2001] 1 ALL ER 991
interest of the public in having access to the information, which will depend on the roles of the data subjects in public life\textsuperscript{91}.

It is submitted that Hong Kong should recognise a public interest defence and have a broader interpretation of journalistic activities so as to strengthen privacy rights and maintain a proper balance between competing interests such as freedom of information and expressions. Useful insight could be drawn from other jurisdictions, particularly the defences of journalistic activities and public interests under the EU and English laws. As admitted by Dr. Marcelo Thompson, online intermediaries are usually faced with a steeper challenge because of the condition of their responsibility\textsuperscript{92}. In implementing a right to de-list in Hong Kong, while on one hand individual’s privacy protection should be strengthened, online intermediaries should also be able to avail themselves of the public interest and newsworthiness defence in relation to any information on their platform regardless of whether it is third-party content or not.

\textbf{Conclusion}

In the era of digitalisation, once a piece of information is posted on the Internet, it is never truly forgotten\textsuperscript{93}. Although there are definitely societal benefits from persistent availability of data, there are significant costs imposed as well. One example is that prolonged retention of data may be detrimental to rehabilitation of individuals\textsuperscript{94}. Potential harm caused by prolonged hosting of publicly available data is enunciated by Professor Lyrissa Barnett Lidsky:

\begin{quote}
“Although Internet communications may have the ephemeral qualities of gossip with regard to accuracy, they are communicated through a medium more pervasive than print, and for this reason they have tremendous power to harm reputation. Once a message enters cyberspace, millions of people worldwide can gain access to it… The extraordinary capacity of the Internet to replicate almost endlessly any message lends credence to the notion that ‘the truth rarely catches up with a lie’.”\textsuperscript{95}
\end{quote}

However, we should be careful in construing our privacy rights in relation to online intermediaries, and should carefully draw the extent and boundary of a right to request intermediaries to take down offending content. It is no longer a valid assertion that all Internet intermediaries are mere conduit or

\textsuperscript{91} Google Spain, para 81
\textsuperscript{92} [Ibid 74], pg. 51
\textsuperscript{94} [Ibid 85]
passive facilitators such that they should not bear any responsibility for any materials they publish. Recent development in the common law breach of confidence action, Strasbourg jurisdiction, and recent Hong Kong cases all show that there could, and in a lot of cases should, be an extension of responsibility of intermediaries in light of their true nature. The new EU Commission Proposal even takes a step further as to entitle individuals a right to request third parties to remove content in the public domain directly.

In light of our constitutional right of freedom of speech, existing legislations and statements by the government and the Office of the Privacy Commissioner, a broad right to erasure of personal data in the public domain similar to that in the new EU regime is unlikely to be applicable in Hong Kong. The proper solution to address the lacunae in privacy laws would be recognising a narrower form of right than the EU regime—to introduce a right to de-list that would enable Hong Kong citizens to request online intermediaries to remove, for example, hyperlinks connecting to personal data in the public domain under certain circumstances. It is regrettable that the AAB and the then Privacy Commissioner have missed the opportunity to clarify the position of Hong Kong laws and the role of Data Protection Principles vis-à-vis online intermediaries in the Do No Evil App and David Webb cases. In any case, these two decisions have clearly provided some basis for a right to de-list applicable to online intermediaries such as Apps and search engines in Hong Kong.

It is proposed that there should be a legislative amendment to the PDPO to explicitly recognise a right to de-list to enhance protection of our privacy rights. A right to de-list would be applicable to online intermediaries that satisfy the three criteria of knowledge, control, and compile criteria. Online intermediaries should demonstrate reasonable efforts in ascertaining whether the third-party content they host has infringed individuals’ privacy rights. These intermediaries can also be judged by regulatory bodies which determine whether they have taken action that is reasonable under the circumstances. The responsibility would be weightier when the Internet intermediaries are notified by either data subjects or regulatory bodies of potentially violation of privacy rights. However, perfect decisions are not expected as it would add excessive burden on online intermediaries and create potential hardship. An approach based on reasonable efforts coupled with the three criteria and public interest defence approach would strike a proper balance between privacy rights and freedom of expression. Extending liability to online intermediaries including database operators by means of recognition of a right to de-list would therefore not be an undue restriction of the right to free speech. It is hoped that the new Privacy Commissioner would consider my proposal and allow Hong Kong citizens to exercise reasonable and adequate control over their personal data in the public domain.