ADMINISTRATIVE APPEALS BOARD

ADMINISTRATIVE APPEAL NO. 15/2019

BETWEEN

X Appellant

and

PRIVACY COMMISSIONER FOR PERSONAL DATA Respondent

Coram: Administrative Appeals Board

- Mr Erik Ignatius SHUM Sze-man (Deputy Chairman)
- Mr Tong Yee-hang (Member)
- Mr Dennis Wong Chiu-lung (Member)

Date of Hearing: 7 and 8 May 2020

Date of Handing down Written Decision with Reasons: 7 August 2020

DECISION

Index

A. Introduction

1. The present appeal arose from a complaint lodged by the Appellant with the Respondent on 24 May 2018 against Google LLC. After investigation, the Respondent made a decision on 19 June 2019 to terminate the investigation. The Appellant appealed against the Respondent's Decision to this Board.

A1. The Incident, the Links & the Search Results

2. The background facts can be summarized as follows. On 2 July 2014, the Police arrested a number of persons for participating in an unauthorized assembly and obstructing police officers ("**the Incident**"). According to the Police, the arrested persons refused to leave after a protest, occupied vehicular roads and blocked the traffic, thereby endangering public safety and order.

3. The Incident together with names and post-titles of the arrested persons, were widely reported in the news and articles. The Appellant's name and his posts held in official bodies were published. It is suspected by the Appellant that a list of the arrested persons and their particulars were disseminated to various online forums.

4. The Appellant subsequently noticed that when a Google search was conducted using his name as keywords, the results ("**the Search Results**") showed links to the said news, articles and online forums ("**the Links**").

A2. The Appellant & Google LLC

5. On 19 October 2017, the Appellant requested Google LLC to delist the Links from the Search Results, on the grounds that the contents of the Links were defamatory, false and not supported by sufficient evidence.

6. After further correspondence, on 1 November 2017, Google LLC informed the Appellant that they had decided not to take action about the Links, and that they encouraged him to resolve any disputes directly with the website owners and individuals who posted the contents.

A3. The Complaint & Investigation

7. On 24 May 2018, the Appellant lodged a complaint against Google LLC with the Respondent ("**the Complaint**").

8. Pursuant to the Complaint, the Respondent commenced investigation by obtaining information from the Appellant, Google (Hong Kong) Limited ("**Google HK**") and Google LLC.

A4. The Decision & the Present Appeal

9. On 19 June 2019, the Respondent informed the Appellant of the Respondent's decision ("**the Decision**") to terminate the investigation

under section 39(2)(d) of the Personal Data (Privacy) Ordinance (Cap. 486) ("**the Ordinance**"), and in accordance with paragraph 8(e) of their Complaint Handling Policy ("**the Policy**").

10. Section 39(2) (under the title: "*restrictions on investigations initiated by complaints*") of the Ordinance provides that:

> "***The Commissioner may*** *refuse to carry out or* ***decide to terminate an investigation*** *initiated by a complaint* ***if*** *he is of the opinion that, having regard to all the circumstances of the case-*
>
> *(a) the complaint, or a complaint of a substantially similar nature, has previously initiated an investigation as a result of which the Commissioner was of the opinion that there had been no contravention of a requirement under this Ordinance;*
>
> *(b) the act or practice specified in the complaint is trivial;*
>
> *(c) the complaint is frivolous or vexatious or is not made in good faith;*
>
> *(ca) the primary subject matter of the complaint, as shown by the act or practice specified in it, is not related to privacy of individuals in relation to personal data; or*
>
> *(d) any investigation or* ***further investigation is*** *for any other reason* ***unnecessary****."*
> *(emphasis added)*

11. Paragraph 8(e) (under the title: "*discretion under section 39(2) to refuse to carry out or decide to terminate an investigation*") of the Policy provides that:

> *"Section 39(1) and (2) of the Ordinance contain various grounds on which the Commissioner may exercise his discretion to refuse to carry out or decide to terminate an investigation. In applying some of those grounds, the PCPD's policy is as follows:*
>
> *[...]*
>
> *In addition, an investigation or* ***further investigation may be considered unnecessary if:***
>
> > *e. after preliminary enquiry by the PCPD,* ***there is no prima facie evidence of any contravention of the requirements under the Ordinance****;"*
> > *(emphasis added)*

12. The Decision was made by the Respondent purportedly based on four grounds. Firstly, it was considered that the Respondent could not pursue the Complaint:

> *"13. According to Google LLC and Google HK [...],* ***Google HK does not exercise any control*** *over the collection, holding, processing or use of personal data in relation to the Google search product,* ***not*** *satisfying the meaning of [']****data user****[']* *under the*

Ordinance.

*14. **As far as Google LLC is concerned, given that it lies outside the territorial jurisdiction of the Ordinance, this office is unable to take enforcement action against it**, even if it is able to control, in or from Hong Kong, the collection, holding, processing or use of personal data in relation to the Links."*
(emphasis added)

13. Secondly, the Respondent considered that there was a lack of evidence to prove that the contents of the Links were inaccurate:

"16. DPP 2(1)(b)(ii) of the Ordinance provides that where there are reasonable grounds for believing that the personal data is inaccurate having regard to the purpose (including [any] directly related purpose) for which the data is to be used, all reasonably practicable steps shall be taken to ensure that the data is erased. The word ['']inaccurate['] is defined in section 2(1) of the Ordinance, which means the data is incorrect, misleading, incomplete or obsolete.

17. The articles posted through the Links revealed that, among other things, [the identity of the Appellant and his post held in official body, and that the Appellant] was arrested by the Police on 2 July 2014. Undoubtedly, your name, post title, and the information on your arrest are factual information which should be verifiable.

18. According to the case of Administrative Appeal No. 32/2004, it is the complainant's duty to provide justification showing that there is a prima facie case of contravention of the Ordinance. In that case, the Administrative Appeals Board decided that: ['']If there is no prima facie evidence of contravention of the Ordinance by the practice or act complained of, the Privacy Commissioner can exercise his discretion to refuse investigation under section 39. The Appellant should bear in mind that complaint about contravention of the Ordinance by others is equivalent to accusation of committing an offence, which is a serious accusation. Therefore, a complaint should have basis, including evidence and justification. The Privacy Commissioner has to consider if there is any basis for the complaint, i.e. prima facie evidence and justification, before deciding whether to investigate...['] In this regard, the onus rests with you as the complainant, to prove that your personal data contained in the articles posted through the Links is inaccurate.

19. Given that ***you refused to state to us whether you were in fact arrested by the Police as mentioned*** *in the articles and online forums concerned [...], there is a lack of evidence to prove that the contents associated with the Links are inaccurate and therefore warrant erasure."*
(emphasis added)

14. Thirdly, the Respondent considered that the right to be forgotten was not applicable, and non-erasure or retention of the data posted through the Links could be reasonably justified:

"20. The Ordinance imposes obligations on a data user to erase personal data. DPP 2(2) provides that all data users must take all practicable steps to ensure personal data is not kept longer than is necessary to fulfil the purpose for which it is (or is to be) used. Nonetheless, the erasure of personal data is considered unnecessary where it is in the public interest (including historical interest) for the data not to be erased.

21. In the present complaint, the Incident was widely reported by the press, and were further disseminated and discussed on various online forums. It aroused wide public concern. We therefore consider that the information on your arrest published through the Links was for journalistic purposes, and there is [no] unlawful interest in displaying the Links.

22. We understand your view that the [']right to be forgotten['] should be established in Hong Kong. However, the Ordinance currently does not explicitly provide an individual with such right. For the sake of discussion, the right to be forgotten under Article 17 of the General Data Protection Regulation (GDPR) gives an individual a right to require organisations / businesses to delete his personal data without undue delay under specified circumstances, including where the personal data is no longer necessary in relation to the purposes for which it is collected. Nonetheless, the right to be forgotten is about empowering individuals' reasonable control over their personal data, not about indiscriminately erasing past events. Neither is it meant to take precedence over freedom of expression and information, albeit the continued existence and

dissemination of the information concerned is prejudicial to the data subject. In this regard, Article 17 of the GDPR explicitly recognises certain exceptions where retention of the data is necessary for exercising the right of freedom of expression and information.

23. In view of the above, the validity of a delisting request should be determined by striking a fair ***balance between the legitimate interest of Internet users potentially interested in having access to the information, and the data subject's fundamental right to privacy and data protection****.*

24. As far as your case is concerned, having made reference to NT1 & NT2 v Google LLC [2018] EWHC 799 (QB) and carefully considered the circumstances of the case, and in particular the following, we are of the view that the right to be forgotten would not be applicable, and non-erasure or retention of the data posted through the Links can be reasonably justified:

(a) The information on your arrest published through the Links ***relates to*** *one or more of the* ***suspected criminal offences****, such as participating in an unauthorised assembly and obstructing police officers in the due execution of their duties. Such information may be* ***sensitive*** *in nature, but it is* ***not intrinsically private*** *in nature.*

(b) The fact that the information on your arrest was widely reported by the press should ***fall within your reasonable***

expectation *as it was a* ***foreseeable consequence of your own actions*** *which might lead to the commission of a criminal offence.*

(c) The information on your arrest is ***not hate speech or libel****.*

(d) There is ***no evidence*** *showing that the information in question is* ***inaccurate, irrelevant or excessive****.*

(e) The matters reported in the news articles i.e. the allegedly unauthorised assembly in the public place in question and the arrests made by the Police have indeed ***aroused wide public concern*** *and continued to* ***form a basis for a great many discussions*** *in society."*
(emphasis added)

15. Fourthly, the Respondent considered that the Appellant's personal reputation was outside the ambit of the Respondent's office:

"25. We note that your primary grievance was against Google LLC for publishing allegedly defamatory information on you (i.e. you were arrested in the Incident) on the Internet by showing the Links in the search result when someone conducts ['']Google search['] using ['][the Appellant's name]['] as search index.

26. You believed that some members of the public would perceive you unfavorably after perusing the information on your arrest published through the Links. You also stated that employers would

normally perform an online search before deciding whether to hire a prospective employee. You were of the view that the publication of the information on your arrest through the Links by Google LLC adversely affected your reputation. In this regard, we would like to cite the following comments from the decision of the Administrative Appeals Board in Administrative Appeal No. 49/2005 which put beyond doubt the ambit of the Ordinance:

> *['] ... the aim of the Ordinance is 'to protect the privacy of individuals in relation to personal data, and to provide for matters incidental thereto or connected therewith.' ... false information and fabricated evidence are not personal data and* ***nor is personal reputation*** *(this office's emphasis). They are not protected by the Privacy Ordinance.[']*

27. We regret to say that we are not in a position to comment on whether the contents associated with the Links are defamatory or whether Google LLC is a publisher of such allegedly defamatory materials generated by its search engines, which is outside the ambit of this office.

28. If you consider that Google LLC has published defamatory information against you, the matter may be resolved through legal channels rather than personal data protection."

16. On 2 July 2019, the Appellant lodged the present appeal against the Decision with the Administrative Appeals Board ("**the Board**").

B. Application for Anonymity Order

B1. Submissions

17. An application for anonymity order dated 2 July 2019 was filed by the Appellant.

18. Pursuant to the Board's directions, both the Respondent and Google LLC filed their respective written submissions in respect of the Appellant's application.

B2. Principles

19. Section 17 (titled "*hearings to be in public except in special circumstances*") of the Administrative Appeals Board Ordinance (Cap. 442) provides that:

> *"(1) Subject to subsections (2) and (3), the hearing of an appeal to the Board shall be in public.*
>
> *(2) **Where the Board hearing an appeal, after consulting the parties to the appeal, is satisfied that it is desirable to do so, it may by order**—*
>
> > *(a) direct that a hearing or part of a hearing shall take place in private and give directions as to the persons who may be present; and*

(b) ***give directions prohibiting or restricting the publication or disclosure*** *to some or all of the parties to the appeal, or to some or all of the persons who may be present, of evidence given before the Board or* ***of any matter contained in any document lodged with the Board or received in evidence by the Board****, whether or not it has given directions under section 14 in respect of any such evidence, matter or document.*

(3) ***In the making of an order under subsection (2), the Board****, without affecting the generality of that subsection,* ***shall in determining whether or not it is desirable to make an order, take into account any views of the parties to the appeal****, including the private interests of and any claim as to privilege by any of those parties.*

(4) For the purposes of this section, any question in relation to a claim by any party as to privilege shall be a question of law." (emphasis added)

20. In *A v Privacy Commissioner for Personal Data* (Administrative Appeal No. 18/2016, Decision dated 21 February 2017), the Board, in determining an application for private hearing and anonymity order, considered and applied previous authorities which addressed the issue (see paragraphs 33-41 on pages 9-17 of the Decision).

21. One of the authorities considered was *Asia Television Ltd v Communications Authority* [2013] 2 HKLRD 354, in which the Court of

Appeal in the course of determination of an application for hearing in camera, laid down the following principles (see pages 362-365):

> *"19. First and foremost, "justice should not only be done, but should manifestly and undoubtedly be seen to be done": R v Sussex Justices, Ex parte McCarthy [1924] 1 KB 256, 259, per Lord Hewart CJ.* ***Open administration of justice is a fundamental principle of common law****: Scott v Scott [1913] AC 417 ; R v Chief Registrar of Friendly Societies, Ex parte New Cross Building Society [1984] 1 QB 227 ; Re BU [2012] 4 HKLRD 417 . It is of great importance, from the perspective of administration of justice, for a number of reasons. The public nature of proceedings deters inappropriate behaviour on the part of the court. It also maintains the public's confidence in the administration of justice. It can result in evidence becoming available which would not become available if the proceedings were conducted behind closed doors or with one or more of the parties' or witnesses' identity concealed. It makes uninformed and inaccurate comment about the proceedings less likely. R v Legal Aid Board, Ex parte Kaim Todner [1999] QB 966, 977E/F-G.*
>
> *20. Second, from the litigants' perspective, open justice also gives effect to their rights to a public hearing guaranteed in article 10 of the Hong Kong Bill of Rights.*
>
> *21. Third, from the public's point of view, open justice, which carries with it the freedom to attend proceedings and to report on them, gives substance to the media's right to freedom of expression*

including the freedom to seek and impart knowledge, guaranteed under article 16(2) of the Hong Kong Bill of Rights. Likewise, it enables the public to enjoy their right to seek and be imparted with knowledge guaranteed under the same article.

22. Fourth, all this means that ***any restriction on open administration of justice*** *necessarily represents a compromise of these important interests, rights and freedoms, and* ***must be justified by considering and balancing all pertinent interests, rights and freedoms****, including in particular those mentioned above.*

23. Fifth, the case law has firmly established that the following considerations or matters do not by themselves justify any restriction on open administration of justice:

> *(1) Publicity of litigation leading to embarrassment and inconvenience: Re Wong Tung Kin [1989] 1 HKLR 93; Ex parte New Cross Building Society, at p.235F.*
>
> *(2) Publicity leading to economic damage, even very severe economic damage: R v Dover Justices, Ex parte Dover District Council and Wells (1992) 156 JP 433.*
>
> *(3) Professional embarrassment and possible damage to profession reputation: Ex parte Kaim Todner, at pp.975H-976C.*

(4) The parties' agreement that the proceedings be held in private: Ex parte Kaim Todner, at p.977C-E.

(5) The mere fact that the subject proceedings etc which gave rise to a judicial review application were held in private: Re The Takeovers & Mergers Panel [1996] 2 HKLR 60 ; Sit Ka Yin Priscilla v Equal Opportunities Commission [1998] 1 HKC 278 .

24. Viewed in terms of the balancing exercise described above, it may be said that the right to privacy underlying some of these considerations or matters is in itself insufficient to justify a departure from the general rule of open justice (see also paragraph 31 below).

25. This is hardly surprising. After all, unwanted publicity, embarrassment and so forth are some of the normal incidence of litigation. They are some of the inevitable consequences of open justice. As a general rule, no one involved in litigation, particularly the initiating party of litigation, can complain. In many but certainly not all cases, if parties desire secrecy, they may, where appropriate, go for arbitration, mediation or some other form of alternative dispute resolution.

26. Sixth, however, open justice is, from the perspective of proper administration of justice, just a means, albeit an important one, to an end, that is, the doing of justice between the parties concerned: Scott v Scott, at p.437; Ex parte New Cross Building Society, at

p.235E. It therefore follows that where open administration of justice in a case would frustrate that ultimate aim of doing justice, it is a most important if not decisive consideration to take into account when balancing the relevant interests, rights and freedoms involved, to decide whether open justice should be restricted, and if so, by what means and to what extent.

27. The case law has very often expressed this in terms of ***a requirement of "necessity"****, that is,* ***where justice would be frustrated if open administration of justice in a particular case is not restricted****, then, to the extent necessary to prevent that from happening,* ***there may be restriction on doing justice openly****.*

28. This requirement of "necessity" is founded on the common law, and has also found expression in article 10 of the Hong Kong Bill of Rights and, in the case of the Court of Final Appeal, section 47(3) of the Hong Kong Court of Final Appeal Ordinance. Article 10 of the Hong Kong Bill of Rights relevantly provides that the press and public may be excluded from a hearing "to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice".

29. Obvious examples here include proceedings involving wards of court or mentally incapacitated persons. Another example is proceedings for the protection of secret process. Scott v Scott, at p.437.

30. All this must be understood in terms of the balancing exercise described above given that different and sometimes competing interests, rights and freedoms are or may be at stake. This is all the more so when quite often, one is concerned with a risk that justice cannot be done (if it is to be administered openly), rather than a certainty that this will be so. In that type of situation, the court's task is to balance that risk (and other relevant interests etc) against other competing considerations and come up with an answer that best serves the situation at hand.

31. Seventh, apart from the interests of justice, there are other similarly important considerations that may justify restrictions on open justice. Thus article 10 of the Hong Kong Bill of Rights also mentions "reasons of morals, public order (ordre public) or national security in a democratic society, or when the interest of the private lives of all parties so requires" as exceptions to the requirement of a public hearing. See, for instance, In re Guardian News and Media Ltd [2010] 2 AC 697 (right to respect for private and family life).

32. Eighth, where justice can be administered openly in the case itself, but to do so would or might jeopardise some right or interest of one or both of the parties outside of the case, whether open justice should be restricted and if so, the manner and extent of restriction, must be considered by conducting the balancing exercise already described. One common example is cases concerning refugees or torture claimants where it is said that the life, limb or liberty of the refugee or torture claimant or their family

is or may be put at risk in the absence of some form of restriction on open justice: R (Kambadzi) v Secretary of State for the Home Department [2011] 1 WLR 1299 ; Re BU (supra).

33. The present case falls within this category of cases. As mentioned, it was not Mr Yu's case that justice cannot be done between the parties in the appeal itself if it were to be heard in open court. Rather, counsel's principal argument was that open administration of justice in this appeal would jeopardise the applicant's right to a fair hearing in the ongoing investigation guaranteed under article 10 of the Hong Kong Bill of Rights. The argument can only be resolved by conducting the balancing exercise described above.

34. Ninth, there are other miscellaneous but by no means insignificant considerations that, if relevant, should be taken into account in conducting the balancing exercise. For instance, the nature of the proceedings is relevant: Ex parte Kaim Todner, at p.978C-D/E. In particular, proceedings by way of judicial review relate to decisions made in the public field, and as a general rule, they must be held in public, as the public has a legitimate interest to be informed about them, unless justice would be denied: Re The Takeovers & Mergers Panel, at p.62D; Sit Ka Yin Priscilla v Equal Opportunities Commission, at p.281D. This is an additional consideration to the general consideration about the media's and the public's right to know based on article 16(2) of the Hong Kong Bill of Rights discussed in paragraph 21 above.

35. Moreover, it is not unreasonable to regard the person who initiates the proceedings as having accepted the normal incidence of the public nature of proceedings: Ex parte Kaim Todner, at p.978D/E-G.

*36. Tenth, **where restriction on open justice is justified, it may take many forms**, depending on how all pertinent interests, rights and freedoms should best be balanced. For instance, in the present case, the applicant asks for a blanket order for the hearing to be held in camera. Alternatively, it asks for a partial censor of the contents of the submissions to be ventilated in open court. Sometimes, a court may impose reporting restrictions on proceedings held in public. At other times, the court may simply **restrict the identification of the parties involved in the proceedings**: In re Guardian News and Media Ltd [2010] 2 AC 697; Re BU." (emphasis added)*

B3. Analysis

22. The Board finds the above line of authorities which gave guidance of the relevant considerations applicable to the present application of the Appellant useful. The Board applies the above considerations in the exercise of the discretion.

23. The restriction in the anonymity order sought by the Appellant concerns his name and particulars which will reveal his identity. Such information is exactly the subject matters of his pursuit and objective in his request to Google LLC and complaint to the Respondent, and finally in the

present appeal. Irrespective of the outcome of this appeal, the Appellant does have a genuine concern and a legitimate purpose to serve to protect his private personal data. It will be an irony and will frustrate the said legitimate purpose of the Appellant if in course of this appeal the hearing of which is open to the public and the Decision also to be published to the public if the very information the Appellant seeks to protect were to be made public. In the eye of justice, the Appellant does have a valid ground in his application.

24. Furthermore, the issues in the present appeal are matters of legal matters, construction of the relevant Ordinance which do not relate to the Appellant's identity or his posts in the official body. The public nor the Respondent and Google LLC simply do not have interest in the context of the appeal to have regard to the above information. In the premises, while the granting of the order sought by the Appellant is important to him, the concealing of such information will have no adverse effect on the integrity of the present Decision of any party or the public.

25. For the above reasons, the Board grants the anonymity order applied by the Appellant and he is only referred to as "X" in this Decision.

C. Grounds of Appeal and Submissions

26. In respect of the substantive appeal, the Appellant filed his grounds of appeal in July 2019.

27. The Respondent filed a statement dated 11 September 2019.

28. Google LLC filed its written submissions dated 3 October 2019.

29. The Appellant filed a statement of response dated October 2019 (without a specific date) to reply to the statement of the Respondent and the written submissions of Google LLC.

30. The Board has considered the grounds of appeal which at the hearing condescend to the issues set out hereinbelow, all the written submissions of the Parties and the oral submissions they made at the appeal hearing. The Board does not propose to set out all the submissions and arguments on the issues raised in detail. At the hearing upon the request of the Board, Counsel for Google LLC prepared a summary of the positions/stances of the parties in relation to the main issues of the appeal ("**the Summary**"), to which the Respondent agrees and the Appellant only wants to add some references of his case. Attached herewith the Summary with the Appellant's added references in red. With the assistance of the Summary it suffices for the Board to set out, in the course of analysis and reasons of the Board herein, the more relevant and important submissions of the parties.

D. Issues

31. Having considered the grounds of appeal and the respective submissions of the parties, as agreed by the parties and set out in the Summary, the following main issues fall to be resolved by the Board:

a. What is the territorial scope of the Ordinance? This is purely a question of law.

b. Whether Google LLC is a "data user" within the definition of the Ordinance?

c. Under this issue whether the criteria of "control requirement" and "processing requirement" are necessary conditions for the application of the Ordinance? The above issue is purely a question of law.

d. Whether there is any "control" of the Google data search engine by Google LLC in Hong Kong?

e. Whether Google LLC has acted in breach of DPP 2(2) and/or section 26(1) of the Ordinance?

f. Whether the "right to be forgotten" is recognized in Hong Kong, and if so the application of the balancing exercise for the right?

32. The other complaints of the Appellant against the Decision of the Respondent such as inaccuracy of the data kept and defamation are not pursued by the Appellant in the appeal.

E. What Is the Territorial Scope/Jurisdiction of the Ordinance

E1. The LRC Report & the OECD Guidelines

33. As stated in the explanatory memorandum to the Personal Data (Privacy) Bill 1995, the Ordinance gives effect to the majority of the

recommendations contained in the report of the Law Reform Commission ("**the LRC**") on Reform of the Law Relating to the Protection of Personal Data published in 1994 ("**the LRC Report**") (see paragraph 34 on page 723 of *Commissioner of Police v Privacy Commissioner for Personal Data* [2012] 3 HKLRD 710).

34. On the one hand, chapter 2.1 (i) (under the title: "*information privacy in the international context*") of the LRC Report provides that one of the international aspects of information privacy of which local legal reforms must be cognisant is "*internationally recognised data protection principles and the development and implications of transborder data flow regulation*". Chapter 2.2 (under the same title) then provides that such recommendations are based on the Organisation for Economic Co-operation and Development ("**OECD**") Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("**the OECD Guidelines (1980)**").

35. Chapter 2.9 (under the title: "*international initiatives to rationalise protection of information privacy*") of the LRC Report provides that the OECD "*is primarily concerned with the economic development of its member states [...] including not only many European countries but also the United States, Australia, New Zealand and Japan*". It also states the initiative to be "*in an effort to introduce a rationalisation of the international regulation of data flows*". The OECD Guidelines (1980) were developed by experts and became applicable in 1980.

36. Paragraph 1a (under the title: "*general definitions*") of the OECD Guidelines (1980) provides for a term, "*data controller*", which means "*a*

party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf". It is explained in paragraph 40 (under the title: "*detailed comments*", and the sub-title: "*paragraph 1: definitions*") that the term "*attempts to define a subject who, under domestic law, should carry ultimate responsibility for activities concerned with the processing of personal data*". Paragraph 16 (under the title: "*basic principles of international application: free flow and legitimate restrictions*") of the OECD Guidelines revised in 2013 ("**the OECD Guidelines (2013)**") further provides that "*a data controller remains accountable for personal data under its control without regard to the location of the data*".

37. On the other hand, chapter 17 (titled "*transborder data flow*") of the LRC Report, which was heavily relied on by the Appellant in advancing his argument on extra-territorial effect of the Ordinance, provides that:

> "*Summary*
>
> *17.1* ***This chapter examines the controls which should be imposed on the transfer of personal data to jurisdictions lacking adequate data protection****, whether or not the transfer is by automated means. It raises the question of the territorial scope of a data protection law in Hong Kong. We conclude that* ***Hong Kong's data protection law should apply to any personal data which is processed or controlled in Hong Kong****, regardless of whether or not the personal data is held within the territory.*

[...]

Territorial scope of data protection laws

17.12 The simplest logical method of regulating data transferred from the territory would be to subject it to the same regulatory framework as that applied within Hong Kong, whether or not the data processing was conducted or controlled in Hong Kong. But giving the law this extraterritorial scope is subject to the constraints of constitutional law. A common law doctrine of uncertain ambit limits the ability of a colonial legislature to enact laws with extraterritorial effect. The basis of this limitation derives from the limited grant of legislative power accorded colonies such as Hong Kong. Hong Kong is only empowered to enact legislation for the "peace, order and good government" of the colony. Laws which do not have a "real and substantial relation" to the colony are vulnerable to being struck down as invalid by the courts. Such a nexus may not be made out merely because the data processed out of Hong Kong relates to a Hong Kong resident. The Hong Kong (Legislative Powers) Order 1986 provides for some limited exceptions which would not encompass data protection. There is also the practical consideration that if the data are not processed or controlled within Hong Kong, effective enforcement action by the local oversight authority is precluded. This is no doubt why other countries not subject to this territory's constitutional limitations have legislated in terms that ensure that effective enforcement remains feasible.

17.13 A few examples will suffice to indicate some of the main approaches taken by other countries in determining the territorial scope of their data protection laws. The French law fixes legal liability on data users involved in even the partial processing of personal data (eg collection) within France. If the processing is carried out by a foreign data user's agent (eg a computer bureau), that agent must be identified in the declaration as the foreign data user's representative and as such is subject to the law. This ensures that legal redress is always available against someone present within the country.

17.14 The UK law focuses not on whether processing takes place within that country, but on whether control over such data is exercised within the UK. This may result in a broader territorial sweep to the UK law, as compared with its French counterpart, in that the UK law applies where control is exercised within the UK, even if the processing is carried out elsewhere. As regards computer bureaus, however, the determining factor is whether the processing is carried out in the UK.

17.15 A further variant is provided by the Netherlands law, whose territorial scope is primarily determined by whether the file is located within the country. Nugter points out that a consequence of this diversity of approaches to territorial application is that of potential overlap. A file located in the Netherlands and processed in France by a computer bureau at the behest of a UK based data controller will be subject to laws of all three countries. Conversely, the application of different tests may result in no law being applied.

17.16 ***In choosing an appropriate criteria to determine the territorial scope of a data protection law for Hong Kong, the two obvious factors are control and processing.*** *We think it important that, in the interests of promoting the continued free flow of data to Hong Kong, Hong Kong not become a data haven, free of effective controls on personal data. To that end, we think it important that, for instance, the data protection law in Hong Kong should continue to apply to a data controller in the jurisdiction, even where the data has been transferred to another jurisdiction.*

17.17 ***There are three ways of providing transborder data protection.*** *The first would be to apply the legislation to processing controlled by a data user within the jurisdiction (as in the United Kingdom). The second would be to apply the provisions where processing of the data had taken place within the jurisdiction (as in France), and the third would be to apply the provisions if the data related to citizens of that country.* ***The sub-committee took the view that a control test should be applied but we have concluded that this needs to be supplemented by the second test, whereby the law would apply to data processed in Hong Kong, whether or not the data controller was based here.*** *This would reassure other countries that Hong Kong would not become a data haven.* ***For example****, the data controller based in France might only be prepared to transfer data to Hong Kong if the data continued to be subject to a data protection law. The French law would cease to protect the data following transfer, as that law lacks a control test. Nor would the control test apply to the processing of data in Hong*

Kong, with the data controller situated in France. The regulatory gap can only be filled by applying the Hong Kong law to data processed here.

17.18 We accordingly recommend that the general provisions of the data protection law should apply to the ***processing of personal data in Hong Kong, whether or not the data controller is in the territory****. Equally,* ***data processing outside Hong Kong which is controlled from within the territory*** *should also be subject to the general application of the law. We note that* ***this approach is in line with Article 4 of the draft Directive.*** *"*
(emphasis added)

E2. The LRC Paper

38. Before the LRC Report was published, the LRC published in 1993 a consultation paper on reform of the law relating to information privacy (**"the LRC Paper"**). Chapter 18 (also titled *"transborder data flow"*) thereof states that:

"SUMMARY

This chapter examines the controls which should be imposed on the transfer of data to countries lacking adequate data protection, whether or not the transfer is by automated means. It raises the question of the territorial scope of a data protection law in Hong Kong. We conclude that ***Hong Kong's data protection law should apply to any data which is controlled in Hong Kong****, regardless of*

whether or not the data is held within the territory.

[...]

DELIBERATIONS

[...]

B. Territorial scope of data protection laws

18.5 The simplest logical method of regulating data transferred from the territory would be to subject it to the same regulatory framework as that applied within Hong Kong, whether or not the data processing was conducted or controlled in Hong Kong. But giving the law this extraterritorial scope is subject to the constraints of constitutional law. A common law doctrine of uncertain ambit limits the ability of a colonial legislature to enact laws with extraterritorial effect. The basis of this limitation derives from the limited grant of legislative power accorded colonies such as Hong Kong. It is only empowered to enact legislation for the "peace, order and good government" of the colony. Laws which do not have a "real and substantial relation" to the colony are vulnerable to being struck down as invalid by the courts. Such a nexus may not made out merely because the data processed out of Hong Kong relates to a Hong Kong resident. The Hong Kong (Legislative Powers) Order 1986 provides for some limited exceptions which would not encompass data protection. There is also the practical consideration that if the data are not processed

or controlled within Hong Kong, effective enforcement action by the local oversight authority is precluded. This is no doubt why other countries not subject to this territory's constitutional limitations have legislated in terms that ensure that effective enforcement remains feasible.

18.6 A few examples will suffice to indicate some of the main approaches taken by other countries in determining the territorial of their data protection laws. The French law fixes legal liability on users involved in even the partial processing of personal data (eg collection) within France. If the processing is carried out by a foreign data user's agent (eg a computer bureau), that agent must be identified in the declaration as the foreign data user's representative and as such is subject to the law. This ensures that legal redress is always available against someone present within the country.

18.7 The UK law focuses not on whether processing takes place within that country, but on whether control over such data is exercised within the UK. This may result in a broader territorial sweep to the UK law as compared with its French counterpart, insofar as the law applies such control is exercised notwithstanding that the processing is carried out elsewhere. As regards computer bureaus, however, the factor is whether the processing is carried out in the UK.

18.8 A further variant is provided by the Netherlands law, whose territorial scope is primarily determined by whether the file is

within the country.

18.9 Nugter points out that a consequence of this diversity of approaches to territorial application is that of potential overlap. A located in the Netherlands and processed in France by a computer bureau at the behest of a UK based data controller will be subject to laws of all three countries.

18.10 ***In choosing an appropriate criterion to determine the territorial scope of a data protection law for Hong Kong, we consider the crucial factor to be whether the data use is controlled within Hong Kong, whether or not the processing is undertaken here. We also gave careful consideration to whether we also wished to fully regulate data processing within Hong Kong where the data controller is outside Hong Kong. We concluded that to do so generally could lead to practical problems.*** *For example, it could be argued that Hong Kong Telecom processes all international telephone calls transmitted through Hong Kong, even though the calls originated and terminated outside the territory. We do not think that to the extent that Hong Kong data users act purely, as processing conduits between other countries, they should be subject to the full force of Hong Kong's data protection regime as regards such data. The application of some of the data protection principles will remain appropriate, however, such as that relating to data security. We therefore recommend that the general provisions of the data protection law apply to the processing of personal data whether or not in Hong Kong, provided the data controller is in the territory. Data process within Hong*

Kong which is controlled from outside the territory should not be subject to the general application of the law, although certain provisions such as those relating to data security may be applied.

18.11 Whilst we consider the control test generally adequate in determining the application of the law to data processors in Hong Kong, to avoid uncertainty we think it should be supplemented in one respect. We recommend that ***data processing involved in the collection of data within Hong Kong should be subject to the application of the law.*** *"Collection" in this context should extend to what may he characterized as the "capture" of data by, for example, an operator keying in instructions to another data user outside Hong Kong. Such collections/captures could perhaps be viewed as evincing the exercise of control over data within Hong Kong. To this extent it may be viewed as a particular application of the control test rather than as a supplement to it."*
(emphasis added)

E3. The EU Directives & the EU GDPR

39. In respect of "*the draft Directive*", as referred to at the end of chapter 17.18 of the LRC Report, chapters 2.13 - 2.14 (under the title: "*international initiatives to rationalise protection of information privacy*") of the LRC Report states:

"2.13 Commission of the European Communities draft Directive
The latest chapter in international efforts to rationalise the legal protection of information privacy is being compiled by the

Commission of the European Communities (the European Commission). ***On 18 July 1990 the European Commission issued a draft Directive concerning the protection of individuals in relation to the processing of personal data.*** *The aim of the draft Directive is to harmonise the different data protection laws presently in force in the European Community, to ensure the free movement of personal data between Member States. The preamble notes that its proposals "give substance to and amplify" those contained in the Council of Europe Convention discussed above.*

2.14 The initial draft Directive represented a "first bid". The European Parliament voted on a large number of amendments in March 1992. ***On 15 October 1992 the Commission issued a substantially revised proposal.*** *The amendments provide for a more flexible and workable framework than its predecessor, whilst continuing to strive for a high level of protection.* ***We have adverted to the revised draft Directive's proposals in formulating our own detailed recommendations on a data protection law."*** *(emphasis added)*

40. The proposed article 4 (titled "*national law applicable*") of the revised draft directive of the European Commission ("**the EU Draft Directive**") states that:

"1. Each Member State shall apply the national provisions adopted under this Directive to all processing of personal data:

(a) of which ***the controller is established in its territory or is within its jurisdiction****;*

(b) of which ***the controller is not established in the territory of the Community****, where for the purpose of processing personal data* ***he makes use of means****, whether or not automatic, which are* ***located in the territory of that Member State****.*

2. In the circumstances referred to in paragraph 1(b) ***the controller must designate a representative established in the territory of that Member State,*** *who shall be subrogated to the controller's rights and obligations."*
(emphasis added)

41. The EU Draft Directive was subsequently adopted by the European Council on 24 October 1995 ("**the EU Directive**") and was eventually repealed by the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ("**the EU GDPR**"). The Appellant relied on the following parts thereof:

a. Preamble 107: "***the Commission may recognise that a third country, a territory or a specified sector within a third country, or an international organisation no longer ensures an adequate level of data protection. Consequently the transfer***

***of personal data to that third country or international organisation should be prohibited, unless the requirements in this Regulation relating to transfers subject to appropriate safeguards**, including binding corporate rules, and derogations for specific situations **are fulfilled**. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.*" (emphasis added); and

b. Article 46(1) (under the title: "*transfers subject to appropriate safeguards*"): "*In the absence of a decision pursuant to Article 45(3), **a controller or processor may transfer personal data to a third country or an international organisation** only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.*" *(emphasis added)*.

E4. The Ordinance

42. Section 4 (titled "*data protection principles*") of the Ordinance provides that:

"***A data user shall not** do an act, or engage in a practice, that **contravenes a data protection principle** unless the act or practice,*

as the case may be, is required or permitted under this Ordinance." *(emphasis added)*

43. Schedule 1 (titled "*data protection principles*") of the Ordinance provides for six data protection principles ("**DPP**"). For instance, DPP 1(1)(a) provides that *"personal data shall not be collected unless the data is collected for a lawful purpose directly related to a function or activity of the data user who is to use the data"*.

44. Section 2(1) (under the title: "*interpretation*") of the Ordinance provides that *"**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**" (emphasis added)*. It also provides that *"processing, in relation to personal data, includes amending, augmenting, deleting or rearranging the data, whether by automated means or otherwise"*.

45. There is no provision in the Ordinance which directly specifies its territorial jurisdiction, i.e. whether a person/entity who controls the collection, holding, processing or use of the data but do so outside of Hong Kong is caught by the Ordinance and subject to its applicability and hence the powers of the Respondent.

46. Section 33(1) (under the title: "*prohibition against transfer of personal data to place outside Hong Kong except in specified circumstances*") of the Ordinance, which is not yet in operation, provides that *"this section shall not apply to personal data other than **personal data the collection, holding, processing or use of which- (a) takes place in***

Hong Kong; or (b) is controlled by a data user whose principal place of business is in Hong Kong *" (emphasis added).* This section was understandably relied on by the Appellant.

47. Section 39(1)(d) (under the title: *"restrictions on investigations initiated by complaints"*) of the Ordinance provides that *"notwithstanding the generality of the powers conferred on the Commissioner by this Ordinance,* ***the Commissioner may refuse to carry out or decide to terminate an investigation initiated by a complaint if none of the following conditions is fulfilled*** *in respect of the act or practice specified in the complaint-*

(i) either-

(A) ***the complainant*** *(or, if the complainant is a relevant person, the individual in respect of whom the complainant is such a person)* ***was resident in Hong Kong****; or*

(B) ***the relevant data user was able to control, in or from Hong Kong****, the collection, holding, processing or use of the personal data concerned,* ***at any time the act or practice was done or engaged in****, as the case may be;*

(ii) ***the complainant*** *(or, if the complainant is a relevant person, the individual in respect of whom the complainant is such a person)* ***was in Hong Kong at any time the act or practice was done or engaged in****, as the case may be;*

(iii) in the opinion of the Commissioner, ***the act or practice done or engaged in****, as the case may be,* ***may prejudice the enforcement of any right, or the exercise of any privilege, acquired or accrued in Hong Kong by the complainant*** *(or, if the complainant is a relevant person, the individual in respect of whom the complainant is such a person); [...]"*
(emphasis added)

E5. Authorities on Interpretation of Statues and on the Ordinance

48. The tools and principles of interpretation of statutes are not disputed in the present appeal which are set out in the following authorities. In *HKSAR v Cheung Kwun Yin* (2009) 12 HKCFAR 568, the Court of Final Appeal laid down the following approach for statutory interpretation (see pages 574-575):

"11. In interpreting a statute, the court's task is ***to ascertain the intention of the legislature as expressed in the language of the statute****. This is of course an objective exercise. The court is not engaged in an exercise of ascertaining the legislative intent on its own. As Lord Reid pointed out in Black-Clawson International Ltd v Papierwerke Waldhof - Aschaffenburg AG [1975] AC 591 at p.613G.*

['] We often say that we are looking for the intention of Parliament, but that is not quite accurate. We are seeking the meaning of the words which Parliament used.[']

12. The modern approach is ***to adopt a purposive interpretation. The statutory language is construed, having regard to its context and purpose.*** *Words are given their natural and ordinary meaning unless the context or purpose points to a different meaning. Context and purpose are considered when interpreting the words used and not only when an ambiguity may be thought to arise. In HKSAR v Lam Kwong Wai (2006) 9 HKCFAR 574 at p.606E, Sir Anthony Mason NPJ stated:*

> *['']The modern approach to statutory interpretation insists that context and purpose be considered in the first instance, especially in the case of general words, and not merely at some later stage when ambiguity may be thought to arise.['']*

See also Medical Council of Hong Kong v Chow Siu Shek (2000) 3 HKCFAR 144 at p.154B-C. As the Court pointed out in Town Planning Board v Society for the Protection of the Harbour Ltd (2004) 7 HKCFAR 1 at p.14A-C, the mischief rule is an early example of the purposive approach. And the purposive approach (including the mischief rule) has been reflected in Hong Kong in s.19 of the Interpretation and General Clauses Ordinance, Cap.1.

13. The ***context*** *of a statutory provision should be taken in its widest sense and certainly* ***includes the other provisions of the statute and the existing state of the law****. See Town Planning Board v Society for the Protection of the Harbour Limited at p.13I-J and Attorney-General v Prince Ernest Augustus of Hanover [1957] AC 436 at p.461.*

14. The purpose of a statutory provision may be evident from the provision itself. ***Where the legislation in question implements the recommendations of a report, such as a Law Reform Commission report, the report may be referred to in order to identify the purpose of the legislation. The purpose of the statutory provision may be ascertained from the Explanatory Memorandum to the bill.*** *Similarly, a statement made by the responsible official of the Government in relation to the bill in the Legislative Council may also be used to this end. See PCCW-HKT Telephone Ltd v Telecommunications Authority (2005) 8 HKCFAR 337 at p.351F-J and Director of Lands v Yin Shuen Enterprises Ltd (2003) 6 HKCFAR 1 at p.15A-H."*
(emphasis added)

49. *HKSAR v Cheung Kwun Yin* was applied in *Commissioner of Police v Privacy Commissioner for Personal Data* [2012] 3 HKLRD 710 (see paragraphs 16-17 on pages 719-720). The Court of Appeal in that case, before construing sections 18-19 of the Ordinance, made the following comments (see paragraph 18 on page 720):

"18. Our attention was also drawn to the general interpretative principle that the Court presumes, unless the contrary intention appears, that the legislator intended to conform to legal policy, which is based on public policy (Bennion on Statutory Interpretation (5th ed., 2008) p.769). Relevant aspects of legal policy for present purposes would include the basic principles that law should serve the public interest (Bennion, pp.779, 786) and that

it should be certain and predictable (Bennion, p.799) and the principle against doubtful penalisation, namely that a person should not be penalised except under clear law (pages pp.784, 825–831)."

50. In *Lawson v Serco Ltd* [2006] ICR 250, the House of Lords, in addressing the issue of the territorial jurisdiction of the Employment Rights Act 1996, applied the following principle (see page 254):

> *"6 The general principle of construction is, of course, that* ***legislation is prima facie territorial****. The United Kingdom rarely purports to legislate for the whole world. Some international crimes, like torture, are an exception. But usually such an exorbitant exercise of legislative power would be both ineffectual and contrary to the comity of nations. [...]"*
> *(emphasis added)*

51. The task of the Board is to apply the above relevant principles of interpretation of statutes and take into account the relevant background of the enactment of the Ordinance, the consultation paper and reports relating to the introduction of the Ordinance, and most importantly the intent reflected by the actual provisions in the Ordinance itself and their effects to ascertain the intention and purpose of the Ordinance in answering the question whether the Ordinance has the intention of applying to data users who is out of Hong Kong and do not control the use of the data in Hong Kong.

52. As submitted by the Respondent, which the board accepts, extra-

territorial application of data protection statues are expressly provided for in statutes of some other jurisdictions. One example is section 5B(1A) of the Privacy Act 1988 in Australia, which applies to acts done, or practice engaged in, outside Australia by an organization, or small business operator, that has an Australian link. Another example is the Data Protection Act 1998 in the United Kingdom, which provides for extra-territorial application where the data controller is established outside the United Kingdom and the European Union, but uses equipment in the United Kingdom for processing the data otherwise than for the purpose of transit. In *Shi Tao v The Privacy Commissioner for Personal Data* (unrep., Administrative Appeal No. 16/2007, 26 November 2007), the appellant lodged a complaint with the Respondent against Yahoo! Holdings (Hong Kong) Limited ("**Yahoo HK**"), which had disclosed to the PRC State Security Bureau account holder information of his email account at the Yahoo! China website (see paragraphs 1-9 on pages 1-2). The Yahoo! China website was wholly owned by Yahoo HK, but operated by a PRC entity and a wholly owned PRC subsidiary of Yahoo HK (see paragraphs 11-16 on pages 3-4). The Board held that Yahoo HK had control over the disclosed information (see paragraph 81 on page 17), but since such information did not constitute "*personal data*", Yahoo HK was not a "*data user*" under the Ordinance (see paragraph 83 on page 17).

53. In that case, the Board considered that since the Ordinance clearly applied, it was not necessary to decide whether it had extra-territorial application (see paragraph 89 on page 19). The Board nevertheless noted as dicta that section 39(1)(d) of the Ordinance, which empowers the Respondent to refuse to carry out or continue an investigation when the case has no connection with Hong Kong, is not a provision dealing with

extra-territorial application of the Ordinance (see paragraph 86 on page 18). Immediately after stating the reasons above, the Board added a footnote that "*the relevant provision in the Ordinance dealing with extra-territoriality appears to be section 33, which is not yet in operation*" (see footnote 7 on page 18).

54. The following three authorities were also relied on by the Appellant:

a. *Oriental Press Group Ltd v Google LLC* [2018] 1 HKLRD 1042. The plaintiffs therein claimed that when a Google search was conducted using "*白粉報*" (translation: "*white powder newspaper*") as the keyword, the results would expressly refer to their Chinese names (see paragraphs 2.2-2.3 on pages 1045-1046). The Court of Appeal affirmed the judge's decision to grant the plaintiffs leave to serve a writ of summons out of jurisdiction against the defendant for defamation, on the grounds that they showed a real and substantial tort had been committed in Hong Kong (see paragraph 3.36 on page 1058);

b. *David M Webb v Privacy Commissioner for Personal Data* (unrep., Administrative Appeal No. 54/2014, 27 October 2015). The complainant therein claimed that when a search was conducted using her name as the keyword, on an online publication in Hong Kong the appellant founded and edited, the results would show links to judgments of divorce proceedings, in which the names of her, her ex-husband and their children were redacted by the court (see paragraphs 2-7 on pages 2-4). The Board affirmed the Respondent's decision to direct the

appellant to remove the links from the website (see paragraphs 8-12 on pages 4-5 and paragraph 61 on page 33); and

c. *HKSAR v Wong Tak Keung* (2015) 18 HKCFAR 62. The appellant therein was convicted of conspiracy to traffic in dangerous drugs, on the evidence that after a courier bought the drugs in Australia from one of the co-conspirators but later reported that they were stolen, the appellant went to Australia, tortured the courier and demanded that he disclosed the whereabouts of the drugs (see paragraphs 2-6 on pages 68-69). The respondent submitted that the Hong Kong court had jurisdiction over a conspiracy to commit an offence abroad, if, according to the approach adopted in a number of English cases, substantial activities constituting the crime occurred within the jurisdiction, even if other essential elements of the offence also occurred abroad (see paragraphs 38-41 on pages 79-80). The Court of Final Appeal, in holding that the Hong Kong court did not have jurisdiction over a conspiracy to commit an offence abroad, held that the said approach had no application in the case where the conspiracy involved the appellant's criminal conduct occurring entirely outside Hong Kong (see paragraph 45 on page 81).

E6. Analysis

55. The Respondent and Google LLC submitted that it covers only personal data of which the "control" (used in the wide sense as defined in the Ordinance) takes place in Hong Kong. The Appellant submitted

otherwise and assert that the Ordinance has extra-territorial effect such that the Respondent has power to enforce the provisions of the Ordinance who does not situates and controls the use of data in Hong Kong. His main reason was that the purpose of the Ordinance, as stated in chapter 17 of the LRC Report, is validated by section 33 of the Ordinance, which gives rise to the extra-territorial jurisdiction of the Ordinance.

56. The wordings used in chapter 17 of the LRC Report and section 33 of the Ordinance are not identical. Chapter 17 provides for *"processing of personal data in Hong Kong"*, whereas section 33(1)(a) provides for *"personal data the* ***collection, holding****, processing* ***or use*** *of which takes place in Hong Kong" (emphasis added)*. Chapter 17 provides for *"data processing outside Hong Kong which is controlled from within the territory"*, whereas section 33(1)(b) provides for *"personal data the* ***collection, holding****, processing* ***or use*** *of which is controlled* ***by a data user whose principal place of business is*** *in Hong Kong" (emphasis added)*.

57. Furthermore, the contexts of chapter 17 of the LRC Report and section 33 of the Ordinance are different. Section 33 deals with the specific transfer of specified data out of Hong Kong, and not general matters of use or control of any data in Hong Kong. In the above different contexts one can easily understand that in section 33 references will be made to persons outside of Hong Kong. Such references do not render any assistance to the Appellant in his argument of extra-territorial effect of the Ordinance, which is a much wider context.

58. The Appellant also relied heavily on some wordings in chapter 17 of the LRC Report, for example, *"Hong Kong's data protection law"* and

"the general provisions of the data protection law", should apply to data controlled or processed in Hong Kong. However, such general wordings were only used in the introductory and concluding sections. In the section which sets out the contents of discussion, for example, in chapter 17.17, the context is an analysis of the three recommended ways of providing transborder data protection, which is very specific and was followed by an example of data being transferred from France to Hong Kong. In the premises, similarly to the Board's observation about the difference between general provisions of data protection law in the Ordinance and section 33 about transborder protection above, the parts in chapter 17 relied on by the Appellant do not assist the Appellant.

59. The Appellant submitted that as the LRC changed its recommendations from control only, as stated in the LRC Paper, to both control and processing, as stated in the LRC Report, it is the intent of the legislature that the territorial jurisdiction of the Ordinance, which is based on the LRC Report, is expanded. The Board disagrees. The change recommended by the LRC, if any, is the recommended scope of provisions on *"transborder data flow"* only. The same limitation appears in the parts of the EU Draft Directive and the EU GDPR relied on by the Appellant. Besides, there is a further requirement under Article 4(2) of the EU Draft Directive for designation by a controller not established in the territory of a representative established therein. The above demonstrate that there is nothing in the LRC Report which supports the contention of the Appellant.

60. The Board considers that the scope and provisions of section 33 of the Ordinance, which deal with a specific area of transborder transfer of data do not suggest any intention of the legislature to wider the

applicability of the Ordinance to persons outside of Hong Kong.

61. In *Shi Tao v The Privacy Commissioner for Personal Data*, it is the Board's decision that the Ordinance applied to the data controlled by Yahoo HK, though managed by its PRC subsidiary. That decision by implication rules out extra-territorial jurisdiction of the Ordinance because otherwise it would have been irrelevant whether Yahoo HK controlled the subject data in Hong Kong.

62. Further, the three cases relied on by the Appellant were decided in completely different contexts and are irrelevant in the present context and hence do not throw any useful light on the issue in the present appeal.

a. The subject matter in *Oriental Press Group Ltd v Google LLC* is a preliminary application for leave to serve out of jurisdiction a writ of summons for defamation, whereas that in the present appeal is a substantive appeal against a decision made in respect of a privacy complaint. The Appellant's initial allegation to Google LLC that the contents of the Links were defamatory, which he no longer pursued, does not render the principles under the tort of defamation applicable in a different context, which is governed by the Ordinance.

b. In *David M Webb v Privacy Commissioner for Personal Data*, the medium in question is a website operated in Hong Kong, and the contents in question are links to judgments redacted by the court, whereas in the present appeal, the medium in question is the Google search engine operated by Google LLC, arguably

operating outside Hong Kong, and the contents in question are links to websites with descriptions of the Incident, without involving any actual legal proceedings, let alone any court order.

c. In *HKSAR v Wong Tak Keung*, the respondent's approach, which was relied on by the Appellant, was held to be not applicable, not to mention the wholly different context of criminal territorial jurisdiction. There is a further significant distinction between those offences under the Ordinance which are substantive, and the offence of conspiracy in *HKSAR v Wong Tak Keung* which is inchoate.

63. In the circumstances, the Appellant has failed to point to any substantive and convincing materials both within and outside of the Ordinance to support his contention in relation to extra-territorial effect of the Ordinance.

64. The general principle that local legislation has no extra-territorial effect unless there are strong pointer to the contrary is a strong one. In the Ordinance itself there is nothing to suggest that the Ordinance would catch and apply its force to persons outside of Hong Kong in the context of privacy protection of data.

65. The Respondent submitted that the difficulty it has in taking enforcement action against a foreign entity and the fact that no provision appears in the Ordinance to deal with that matter mitigate against any extra-territorial effect of the Ordinance. That consideration is a strong indication against extra-territorial effect since it will be frivolous for the Respondent

to serve any enforcement notice on foreign entities who has no operations in Hong Kong, not to speak of further steps concerning criminal sanctions.

66. For the above reasons, the Board finds that the scope/territorial jurisdiction of the Ordinance covers only persons being data user who has operations controlled in or from Hong Kong.

F. Whether the Application of the Ordinance Is Based on the "Control Requirement" and/or the "Processing Requirement"

67. The issue arises from the broad ground of appeal no. 2 of the Appellant. The Appellant submitted that the Control Requirement and the Processing Requirement are both sufficient requirements under the Ordinance such that if Google LLC's operations satisfy either one of the two requirements which take place in Hong Kong then Google LLC has operations within Hong Kong so as to be caught by the scope of the Ordinance. By processing requirement the Appellant means whether there is a "real and substantial" processing of the data (which covers collection, holding, processing and use) in Hong Kong, which is a wider meaning given to the word "processing". The Respondent submitted that the Control Requirement is the sole test whereas Google LLC submitted that both requirements form the necessary requirements so that both have to be operated in Hong Kong.

68. To resolve this question of law, the basic provision which need to be understood is the interpretation of "data user" in section 2(1) of the Ordinance which defines the term as *"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" (emphasis added).

69. Another provision which is of relevance is section 39(1)(d)(i)(B) of the Ordinance which sets out some grounds on which the Respondent may refuse to carry out investigation or terminate investigation, if *"none of the following conditions is fulfilled in respect of the act or practice specified in the complaint – (B) the relevant data user was able to control, in or from Hong Kong, the collection, holding, processing or use of the personal data concerned".*

70. Though the word "control" is not defined in the Ordinance, section 2(1) does define "processing" as *"in relation to personal data, includes amending, augmenting, deleting or rearranging the data, whether by automated means or otherwise".*

71. From the above sections of the Ordinance, it is obvious that processing has a much restricted and narrower meaning than controlling. The control test also accords with the definition of data user which should be the criterion of the territorial competence of the Ordinance. The Appellant's contention that either "control requirement" or "process requirement" will be sufficient to satisfy the territorial requirement is without any proper basis. It is even more far fetch for Google LLC to assert that both requirements need to be satisfied before the Ordinance catches the operation. The Board finds that the submission of the Respondent on this issue is well founded and that the proper test is solely the "control requirement".

72. In passing, the Board would also indicate its agreement with the submission of the Respondent that practically it will be difficult to dissect the data cycle at different stages for the purpose of applying different Data Protection Principles and provisions of the Ordinance to different stages. That adds to the illogic of treating the processing requirement as a sufficient requirement or that both control and processing requirements need to be satisfied in the context of territorial jurisdiction of the Ordinance.

G. Whether Google LLC Lies Outside of the Territorial Jurisdiction of the Ordinance

73. It is not in dispute that Google search is operated by Google LLC and not Google HK. As submitted by Google LLC, Google LLC does not have any establishment or office in a company based in Hong Kong.

74. As submitted by Google LLC, which the Board accepts, Google search is a search engine which helps web users to find websites they are likely to be interested in. Google LLC operates Google search in three ways: crawling, indexing and serving of results.

a. Crawling: Google LLC uses a software called crawler. The crawler first sends requests to web servers for the contents of the websites the web servers host. The operators or publishers of the websites then respond, say by accepting the requests and providing all or part of the contents, or by refusing the requests.

b. Indexing: Google LLC compiles indexes for the crawled contents. As crawling is an ongoing process, any updates

example, when the operator or publisher of a website changes from accepting to refusing the request from the crawler, the contents of the website will be removed from the corresponding indexes.

c. Serving of results: When a user conducts a Google search using a keyword, the algorithms of the search engine will look the keyword up in the indexes and find the relevant contents. The results returned to the user will include a list containing hyperlinks to, and titles of, the websites, as well as snippets of the contents of the websites in which the keyword appears.

75. The uncontradicted evidence which the Board accepts is that no data centre, crawling and indexing equipment, and Google search server is located or installed in Hong Kong. Its data centres in Asia are located in Singapore and Taiwan. The processing of a browser's search command is conducted by the search engine which is also installed outside Hong Kong. The availability of search results on the website of Google HK is not a significant factor, because the majority of the search process, as identified above, takes place via facilities and equipment outside Hong Kong.

76. Overall, the Board is satisfied that Google LLC decides on the contents and use of personal data under Google search, through its data centres, crawling and indexing equipment, Google search server and engine, all installed or located outside Hong Kong.

77. This factual issue of control by Google LLC from outside of Hong Kong is not at the heart of the appeal and arguments of the parties. The

positions of the Respondent and Google LLC are consistent to the effect that Google LLC has no presence in Hong Kong. The Appellant does not seriously dispute the Respondent's findings that,

(a) Google HK, though a subsidiary of Google LLC, is a different legal entity from Google LLC; and

(b) The function of Google LLC is to act as operator and administrator of the services of the internet search engine whereas Google HK only serves to provide marketing and support of the Hong Kong businesses.

(c) All the evidence collected and found by the Respondent in the course of its investigation points to the conclusion that all operations of Google LLC in relation to the internet search engine are performed outside of Hong Kong and Google LLC simply has no presence in Hong Kong.

The above conclusions from the evidence obtained by Google LLC are simply not contradicted by the Appellant who has produced no contrary evidence.

78. At the hearing the Appellant simply submitted that the domain of "google.com.hk" is registered by Google (HK) Limited and hence Google HK should have control over the subject data. The Board finds that there is no merit in the said contention of the Appellant which is not supported by any evidence. The domain of "google.com.hk" has nothing to do with the identity of the person who controls the operation of the search engine.

In light of the evidence obtained by the Respondent that it was Google LLC (and not Google HK) which operates the search engine outside of Hong Kong, the Board agrees with the Respondent on this issue without hesitation.

79. By reason of the above analysis the Board finds that:

(a) The Ordinance does not apply to a foreign person or entity who has no operation controlled within or from Hong Kong since the Ordinance does not have extra-territorial effect;

(b) As a matter of fact, Google LLC is not situated and does not have any operations in Hong Kong;

(c) The jurisdiction and power of the Respondent are limited and do not extend to regulate and control the conduct of a foreign body such as Google LLC whose operations are not controlled within or from Hong Kong;

(d) Hence, Google LLC does not fall within the scope of "data user" under the Ordinance.

80. The above conclusions and findings are sufficient to dispose of and dismiss the appeal. The above conclusion is actually the very reason why the Respondent could not pursue the Appellant's complaint under the Ordinance as explained in paragraph 15 of the Respondent's Decision. The Board knows that the Respondent is reviewing the above effect of the Ordinance which for laymen including the Appellant may feel aggrieved.

It is hoped that the Ordinance can be reviewed as to its extra-territorial effect and applicability to persons operating abroad in light of the borderless internet world, sooner the better, with the assistance of the Respondent.

81. However, since the other grounds of appeal were raised by the Appellant and arguments were heard at the appeal hearing, the Board will discuss and gives its views on the other issues raised in the appeal briefly.

H. Whether There Is Collection of Data in Hong Kong

82. On this question, the Board finds that for the reasons given above that the operations of Google LLC all take place outside of Hong Kong and that collection of data on the websites through the internet needs not be done physically in Hong Kong, there is no "collection of data" in Hong Kong.

I. Whether There Is Processing or Holding of Data in Hong Kong

83. For the reasons given above, the Board also finds that there is no processing or holding of data in Hong Kong.

J. Whether Google LLC Is a User of Data

84. Though Google LLC is not caught by the Ordinance by reason of the territorial limitation of the Ordinance as found hereinabove, subject to the above, Google LLC clearly otherwise falls within the definition of data user under section 2(1) of the Ordinance. That is because Google LLC

uses the data collected which can identify the subjects for display in its search engine function. From that angle but for the fact of the Ordinance not applicable to Google LLC by reason of the jurisdictional issue, Google LLC would have been a data user under the Ordinance.

K. Whether Google LLC Acted in Breach of DPP 2 or Section 26

85. By reason of the Board's conclusion on the issue of extra-territorial effect of the Ordinance, it is strictly not necessary for the Board to express any views on whether Google LLC acted in contravention of DPP2 or in breach of section 26 of the Ordinance for failing to erase the personal data of the Appellant from the search engine upon his request. Furthermore, since any concrete conclusions on the above matters may affect the reputation of both the Appellant and Google LLC, there is more the reason for the Board to refrain from making any findings as a matter of dicta. However, since the parties have made full submissions on the issue, the Board will briefly address the legal issues of the "right to be forgotten" and application of the 13 criteria set out in the UK case of NT1 & NT2.

86. DPP 2(2) (under the title: "*accuracy and duration of retention of personal data*") in schedule 1 of the Ordinance provides that:

> "*All practicable steps must be taken to ensure that personal data is not kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data is or is to be used;*"

87. Section 26(1) (under the title: "*erasure of personal data no longer required*") of the Ordinance provides that:

> "*A data user must take all practicable steps to erase personal data held by the data user where the data is no longer required for the purpose (including any directly related purpose) for which the data was used unless—*
>
> *(a) any such erasure is prohibited under any law; or*
>
> *(b) it is in the public interest (including historical interest) for the data not to be erased.*"

88. In *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (C-131/12, 13 May 2014) ("***Google Spain***"), the complainant, a Spanish national, lodged a complaint with AEPD, the Spanish Data Protection Agency, against a publisher of a daily newspaper circulated in Spain, Google Spain and Google Inc. His complaint was that when a Google search was conducted using his name as the keyword, the results showed links to two pages of the newspaper, which contained an announcement for an auction organized following attachment proceedings for the recovery of social security debts owed by him. His requests were that the newspaper, Google Spain and Google Inc. should take steps to ensure that the personal data relating to him no longer appeared. The AEPD rejected his complaint against the newspaper, but upheld those against Google Spain and Google Inc..

89. As a result, Google Spain and Google Inc. brought actions before the Spanish National High Court and claimed that the AEPD's decision should be annulled. The Spanish National High Court then referred questions to the Court of Justice of the European Union. The Court of Justice of the European Union, inter alia, laid down a general principle that if, following a search made on the basis of a person's name, the list of results displays a link to a web page which contains information on the person in question, that data subject may approach the operator directly and, where the operator does not grant his request, bring the matter before the competent authorities in order to obtain, under certain conditions, the removal of that link from the list of results.

90. In *NT1 & NT2 v Google LLC* [2019] QB 344, the two claimants sought, inter alia, orders for the removal of details of their offending, convictions and sentences from Google search results, on the basis that the information, in particular concerning their spent convictions, was old, out of date, irrelevant, of no public interest and/or otherwise an illegitimate interference with their data protection and/or privacy rights. The Queen's Bench Division of the English High Court of Justice applied part II (titled "*list of common criteria* ("**the Criteria**") *for the handling of complaints by European data protection authorities*") of the Guidelines on the Implementation of [*Google Spain*], adopted on 26 November 2014 by a working party established under the EU Directive. The Criteria are as follows (see also "*comments*" in part II, which provide guidance on the application of the Criteria):

"*1. Does the search result relate to a natural person – i.e. an individual? And does the search result come up against a search on the data subject's name?*

2. *Does the data subject play a role in public life? Is the data subject a public figure?*

3. *Is the data subject a minor?*

4. *Is the data accurate?*

5. *Is the data relevant and not excessive?*

   a. *Does the data relate to the working life of the data subject?*

   b. *Does the search result link to information which allegedly constitutes hate speech/slander/libel or similar offences in the area of expression against the complainant?*

   c. *Is it clear that the data reflect an individual's personal opinion or does it appear to be verified fact?*

6. *Is the information sensitive within the meaning of Article 8 of the Directive 95/46/EC?*

7. *Is the data up to date? Is the data being made available for longer than is necessary for the purpose of the processing?*

8. *Is the data processing causing prejudice to the data subject? Does the data have a disproportionately negative privacy impact on the data subject?*

9. *Does the search result link to information that puts the data subject at risk?*

10. *In what context was the information published?*

    a. *Was the content voluntarily made public by the data subject?*

    b. *Was the content intended to be made public? Could the data subject have reasonably known that the content would be made public?*

11. *Was the original content published in the context of journalistic purposes?*

12. *Does the publisher of the data have a legal power – or a legal obligation – to make the personal data publicly available?*

13. *Does the data relate to a criminal offence?*"

91. The privacy law as codified in the Ordinance is a self-contained legislation in Hong Kong. The relevant provisions governing the protection of data subjects are set out in the terms under DPP2 and section 26 of the Ordinance. The "right to be forgotten" which contains a concept

which has meanings of its own does not find its way into the Ordinance. It will require very persuasive authorities in similar legislative situation as in Hong Kong to succeed importing such an independent right into the Ordinance. The Appellant's contention and reliance on the above authorities do not surmount the above hurdle. The Board agrees with Google LLC's Senior Counsel's submission that there is no such independent right in Hong Kong.

92. Though not an independent doctrine on its own right in law, the right to be forgotten is not totally irrelevant in the context of DPP2 and section 26 of the Ordinance. It is relevant to the extent that the concept may be applicable in the course of due consideration of the application of DPP2 and section 26. Hence, the 13 criteria in UK cases of NT1 and NT2 would thus still be relevant consideration in appropriate cases under the Ordinance.

L. Conclusion

93. In conclusion, for the reasons stated in this Decision, the Appellant's appeal is dismissed.

94. At the end of the appeal hearing, both the Respondent and Google LLC indicated that they would not seek costs against the Appellant in any event. In the circumstances, the Board makes no order as to costs of the appeal.

95. It remains for the Board to thank all parties and their representatives for their assistance to the Board. Ms. Cindy Chan, Counsel for the

Respondent, and Mr. Abraham Chan SC, Counsel for Google LLC have presented their clients' cases with clarity and skills. This is particularly helpful to the Board as on different issues the parties have divergent stances. The Appellant had a difficult task acting in person and yet he discharged his job as an advocate for himself with admirable effectiveness for which the Board is particularly grateful.

(signed)
(Mr Erik Ignatius SHUM Sze-man)
Deputy Chairman
Administrative Appeals Board

AAB NO.15/2019 – HEARING ON 7-8 MAY 2020
COMPARISON TABLE OF PARTIES' POSITIONS ON ISSUES IN QUESTION

	Google LLC's ("GL") arguments	**Privacy Commissioner's ("PC") position**	**Appellant's ("X") position**
	Issue 1. Territorial scope of the Personal Data (Privacy) Ordinance ("PDPO")		
1.	Control Requirement is a necessary condition. Same as PC Different from X	Control Requirement is a necessary condition. Same as GL Different from X	Control Requirement is a sufficient condition. Different from GL or PC.
2.	Processing Requirement is a necessary condition. Different from PC Same as X	Processing Requirement is NOT a condition. Different from GL or X	Processing Requirement is a sufficient condition. Same as GL Different from PC.
3.	Need to satisfy BOTH Processing Requirement AND Control Requirement to establish jurisdiction. Different from PC or X	Only need to satisfy Control Requirement (but not the Processing Requirement). Different from GL or X	Only need to satisfy EITHER the Processing Requirement OR the Control Requirement. Different from GL or PC

4.	ONLY those specific act(s) or practice(s) taking place in HK will be subject to the specific relevant DPP or provision of the PDPO covering that act or practice.	Neutral. But PC envisages practical difficulties in dissecting the data cycle in different stage and then applying different DPP/ PDPO provisions.	N/A. Reference: sections 44-45 of Appellant's reply statement
	Issue 1A. The meaning of "processing" under the Processing Requirement		
5.	"Processing" has a narrow definition in the PDPO, covering only "amending, augmenting, deleting or rearranging data" and thus, only acts which falls within this narrow definition taking place in HK will fall within the jurisdiction of HK. Different from PC and X	Wider definition of "processing" i.e. should be construed to cover collection, holding, processing and use of data. Different from GL Similar to X	No definitive view X relies on the definition of the "processing" under the PDPO – processing cover automated means or non-automated means under the PDPO. X also relies on *Google Spain* and the 1995 EU Directive to say GL's search engine falls within the meaning of "processing" under 1995 EU Directive. Reference: sections 46-54 of Appellant's reply statement
	Issue 2. Whether there is any control in or from HK?		
6.	No. The search engine is controlled by Google LLC, which is located outside of HK. Same as PC Different from X	Same as GL Different from X	At hearing, X says that the domain name "google.com.hk" is registered by Google (HK) Limited with the HKDNR. Hence, Google HK has certain control on the data cycle in HK. Reference: sections 141-146 of Appellant's reply statement

	Issue 3A. Whether there is collection of data in HK?		
7.	No collection. Applying the CA's reasoning in ***Eastweek Publisher***, Google has no intention to identify any particular individual at all. Different from PC and X	There is collection of data, and ***Eastweek*** is not applicable because name is collected. Different from GL Same as X	X says the crawling of website by GL happen in HK.GL's crawler needs to go to the website in HK, say Ming Pao, to augment / rearrange such data. Different from GL. But X has not expressly whether X agrees with the PC. Reference: sections 58 and 69 of Appellant's reply statement
	Issue 3B. Whether there is processing or holding of data in HK?		
8.	No. The search engine is installed outside of HK and there is no data centre in HK so there is no processing or holding of data in HK. Same as PC Different from X	Same as GL Different from X	X says the crawling of website by GL happen in HK. GL's crawler needs to go to the website in HK, say Ming Pao, to rearrange such data. Search results are tailored for HK internet users, and hence the search results is specifically arranged in HK. Search results could be distributed via a .hk domain name, ie. www.google.com.hk. Different from GL and PC

	Issue 3C. Whether there is any use of data in HK?		
9.	No use in HK ("use" under the PDPO does not extend to the mere search, retrieval and display of data on a computer screen where nothing further will be done with it. Different from PC and X	PC agrees with X that the meaning of "use" of personal data includes data displayed to internet users in HK. Different from GL Same as X	X says GL uses the search results in HK by displaying, publishing and making available X's personal data to internet users in HK. Different from GL Same as PC Reference: section 78 of Appellant's reply statement
	Issue 4. Whether Google is a "data user"?		
10.	No. Not enough control to be considered data use. It is the operator/publisher of the online news articles/posts which have control. GL cannot change the configuration of the website covering the contents in question. Different from PC and X	Different from GL Same as X In addition to X's points, more recent cases overseas (in EU and British Columbia) held that Google is not a passive website in providing information to internet users.	Different from GL Same as PC X relies on defamation cases to support the argument that GL has certain control over data processing involved during the search process and hence is capable of being a data user under the PDPO. X also says a person "either alone or jointly or in common with other persons" are considered as data user. GL may not be the sole data user, but it is wrong to say GL has no control.

	Issue 5. Whether there is breach of DPP 2 and Section 26 of PDPO?		
11.	DPP2(1) No breach. No evidence of inaccurate data. S.26 No breach. Purpose of Google Search is to provide means and assistance for members of the public to find information on the internet. This purpose has not been "completed" or "fulfilled", and is still on-going as long as information is available on the internet.	DPP2(1) Same as GL and X Agreed at hearing that there is no breach of DPP2(1) re inaccurate data. S.26 Different from GL.	DPP2(1) Same as GL and X Agreed at hearing that there is no accurate data, therefore DPP2(1) does not apply. S.26 Different from GL. Similar to PC. There is breach.
	Issue 6. Whether the "right to be forgotten" ("RtbF") should be recognized in HK?		
12	Right to be forgotten should NOT be recognized in HK without specific legislative amendment. Different from PC and X	Different from GL Same as X There is a "right to be forgotten". Although at hearing, PC agreed that there is no general right and can only rely on DPP2 and s.26 ***Google Spain*** is applicable in HK, as section 26 and DPP 2 were drafted based on 1995 EU Directive. The question is whether the links in question, should be delisted after considering the 13 criteria set out in the UK case of ***NT1 & NT2***.	Same as PC Different from GL Reference: sections 95-98 of Appellant's reply statement

	Issue 7. The application of the balancing exercise for RtbF		
13	After considering the 13 criteria set out in the UK case of ***NT1 & NT2***, the present case is not a suitable case for a de-listing order. Same as PC Different from X	Same as GL. Different from X	Different from GL and PC. Please see refer para 86-91 of the Grounds of Appeal.