Law Drafting Competition 2023

First runner-up

TSOI Cheuk Ling

Topic 1: Private information on Internet

Legislative Proposal Outline

1. Introduction:

In recent years, the usage of cookies in websites and social media applications has surged. However, this gives rise to personal privacy concerns, as cookies and other related website trackers can remember and share sensitive information without the user's informed consent. Hence, this Legislative Proposal seeks to amend the Personal Data (Privacy) Ordinance (Cap. 486) **("PDPO")**, so as to

(a) Expand on the interpretation of personal data;

(b) Amend the consent requirement for the use of cookies or personal data in direct marketing; and

(c) Expand the scope of liability for data processors or other third parties.

2. Justification:

(I) Growing use of cookies and trackers in targeted advertising

Known as 'a small computer file stored in a website user's device'[1], cookies are often used by website operators to track online activities. Generally, cookies can be classified based on their time span[2], sources[3] and purpose of use.[4] With the growing use of targeted advertising[5], there is increasing risk of data privacy breach, as third-party marketing cookies can privately monitor the user's activities and interests through various websites. While flash cookies can bypass the browser's settings, super cookies can be installed in obscure places and duplicate themselves to avoid being deleted.[6] Over time, these cookies allow advertising companies to generate profiles of the users and deliver specific advertisements by compiling the user's data through algorithms. Although Google announced the upcoming phasing out of third-party cookies in 2020, implementing regulations for cookies or website trackers is still crucial, as advertisers may adopt fingerprinting or other tracking technologies to collect the user's personal information.[7]

(II) Existing regulatory regime

Insofar, the PDPO only regulates the collection of personal data for direct marketing purposes, such as requiring the user's consent before collecting the data.[8] In fact, there is no specific clauses prohibiting the use of cookies or other privacy intrusive online tracking tools in the PDPO.[9]

---

[1] Stephen Kai-yi Wong, 'Cookies – Ever Your Choice?' (2019) Industry Insights <https://www.hk-lawyer.org/content/cookies-—-ever-your-choice> accessed 20 January 2023

[2] This includes session cookies that lapse when the user closes the browser and persistent cookies that stay on the hard drive until the user deletes them.

[3] Under this category, this includes first-party cookies and third-party cookies. While first-party cookies are placed directly on the website when the user visits the website, third party cookies are installed by a third-party advertiser or an analytic system.

[4] See Richie Koch 'Cookies, the GDPR, and the ePrivacy Directive' (*GDPR.EU*, 9 May 2019) <https://gdpr.eu/cookies/> accessed 23 January 2023

[5] Alex Dixie and Gigi Cheah, 'Global Cookie Review' (2022) <https://www.twobirds.com/-/media/new-website-content/pdfs/insights/2022/global/bird-bird-global-cookies-review-winter-2022-final.pdf> accessed 30 January 2023

[6] See Office of the Privacy Commissioner for Personal Data, Hong Kong, 'Online Behavioural Tracking' (2014) <https://www.pcpd.org.hk/english/publications/files/online_tracking_e.pdf> accessed 25 January 2023

[7] Alex Angove-Plumb, 'Browser fingerprinting and the death of cookies' (CHOICE, 26 January 2022) <https://www.choice.com.au/consumers-and-data/data-collection-and-use/who-has-your-data/articles/browser-fingerprinting-and-death-of-third-party-cookies> accessed 31 January 2023

[8] Personal Data Privacy Ordinance Cap. 486 s35C

[9] Jojo Y.C. Mo, "Cookies and Browser-Generated Information: The Challenge in Hong Kong Under

Although the Data Protection Principles **("DPPs")** in the PDPO address the use of cookies and website trackers[10], they only provide guidelines and recommendations for good practice.

Regarding the use of cookies and online trackers, website operators are recommended to:[11]

- Clearly state the type of information collected;
- Notify users and explain the details of the information stored in third-party cookies, the objectives for collecting the information and the method of collection; and
- Set out whether the websites permit the user's access if they reject cookies and the resulting consequences. If it is not possible to deactivate online tracking while using the website, explanation must be given to the website users.

For behavioural information, website owners are recommended to:[12]

- Fix a reasonable expiry date for the cookies;
- Encrypt the information stored in the cookie if appropriate; and
- Stop using techniques that ignore the browser settings on cookies, unless they allow website users to deactivate the cookies or reject the use of cookies.

As shown above, the rules regarding cookies and online trackers are non-mandatory and dispersed in multiple guidelines. Hence, in order to improve data privacy and protect commercial interests, the PDPO should be amended to include statutory regulations against cookies and website trackers.

(III) Other jurisdictions

In comparison, most overseas countries recognise cookies as part of personal data and incorporates cookies law under data privacy legislation.

European Union (EU)

---

the Personal Data (Privacy) Ordinance" Statute Law Review, 2017, Vol. 38, No. 1, 63, 68

[10] See DPP1(3)

[11] See Office of the Privacy Commissioner for Personal Data, Hong Kong, *Guidance for Data Users on the Collection and Use of Personal Data through the Internet* (Guidance Note, 2019) p.2

[12] *Ibid* 6

Enforced in 2018, the General Data Protection Regulation **("GDPR")** covers regulation of cookies. According to recital 30 of the GDPR, if online identifiers, such as cookie identifiers, can identify an individual, they are regarded as person data and are regulated under the GDPR. Additionally, the ePrivacy Directive and the Guidelines by the European Data Protection Board provide that the user's consent must be acquired before installation on the user's device.[13]

Besides, in the case C-673/17, the Court of Justice of the European Union held that before website operators launch additional cookies, the user must give express approval by clicking the 'consent' checkbox. For pre-ticked checkboxes, they cannot satisfy the consent requirement. This allows users to exercise more control over the option of sharing their personal data.[14]

Moreover, the upcoming ePrivacy Regulation, which replaces the ePrivacy Directive, provides stricter regulations as to the use of cookies. Under Article 8 of the ePrivacy Regulation, the use of cookies is banned unless they are required for providing essential services, or that a clear consent has been obtained from the user. Besides, there are further restrictions to using cookie walls or pre-ticked boxes.

United Kingdom (UK)

Similar to EU's GDPR, UK's General Data Protection Regulation (**"UK-GDPR"**) features strict regulations against cookies and third-party trackers. For example, website operators must procure the users' consent before tracking their personal data. Apart from UK-GDPR, the amended Data Protection Act 2018 includes legislation regarding cookies and third-party trackers. With the implementation of mandatory rules, it grants UK users the right to erase unnecessary cookies or collected personal data.[15]

California

---

[13] Joshua Chu, "Latest Legal Update Express | Internet of Things Series | Cookies & Law | Comparing Regulations Governing Cookies on the Internet across the Globe" (2021) <https://www.hk-lawyer.org/content/latest-legal-update-express-internet-things-series-cookies-law-comparing-regulations> accessed 28 January 2023

[14] *Ibid* 1

[15] *Ibid* 1

According to the California Consumer Privacy Act, 'persistent cookies' are regarded as personal information, regardless of whether the user can be identified personally under Section 1798.140(o)(1)(A). Moreover, business should notify consumers before collecting their personal data under Section 1798.100(b).[16]

Japan

Differing from EU and UK, Japan's cookie regulation targets the companies' use of cookies in collecting personal data. Before cookies are used in the websites, companies must obtain the users' consent. Besides, if third party cookies are used to form individual profiles, companies must explain how the profiles are made.

In 2020, the Personal Protection Commission proposes an Amendment and introduced the concept of Related Personal Information. If the third party can use cookies to pinpoint an individual, the cookies will be regarded as constituting Related Personal Information. They cannot be given to a third party unless the provider has obtained the individual's consent.[17]

[16] Tim Gole and Jen Bradley, 'A Guide to Internet Cookies' (Gilbert + Tobin, 28 January 2022) <https://www.gtlaw.com.au/knowledge/guide-internet-cookies> accessed 31 January 2023

[17] *Ibid* 1

3. Contents of the proposal:

The draft preliminary sections of the Bill are as follow:

(I) Expanding interpretation of 'personal data'

Under s2 of the PDPO, data is only regarded as personal data if it is accessible, processable and associated with a living individual. Moreover, the data can be used to verify the individual's identity directly or indirectly in a reasonable manner. In determining whether the data constitutes personal data, the relevant case circumstances will be considered.

There are mixed verdicts as to whether cookies or other online identifiers are considered personal data. In Case No 2006C14, the Commissioner held that cookies containing the individual's English name and her website history constituted personal data under the PDPO. However, in case AAB No. 16/2007 and No. 25/2012, the Administrative Appeal Board ruled that an IP address and the user's registered email address does not constitute personal data. Thus, it can be deduced that cookies may not be considered as personal data, but only as browsing history of computer users. As the PDPO only concerns personal data, this may lead to difficulties in regulating cookies under the legislation, due to its ambiguous position.

Hence, with reference to the definition provided in GDPR[18], it is proposed that the definition of 'online identifiers' should be added in order to better regulate the usage of cookies under the PDPO. Furthermore, the definition of 'personal data' should be expanded to include all data gathered from online identifiers, such as persistent cookies.

(II) Changing the requirement for consent

Under s35A of Part VI A of the PDPO, consent is defined as "an indication of no objection to the use or provision." Although the Privacy Commissioner viewed that the user's silence does not amount to consent, this alone does not offer adequate protection to the web users or data subjects. Under the current system in HK, if the user` does not show his or her objection in the consent box, this may constitute consent.

---

[18] General Data Protection Regulation (GDPR) Article 4

Moreover, consent would be found if the user's browser accepts cookies automatically. Hence, it is proposed that the consent requirement should be changed from 'indication of no objection' to informed consent', with reference to EU's Data Protection Directive. According to Article 2(h) of the Data Protection Directive, it states that a valid consent requires a '(i) freely given, (ii) specific, (iii) informed, and (iv) indication of wishes', and that the user must agree to the processing of personal data before installing tracking cookies. Furthermore, reference can be made to UK's approach. In its Directives relating to data protection, it proposes that for cookies that are more intrusive, a higher degree of consent is required before installation.[19]

Therefore, it is proposed that the user's consent should be obtained before cookies or website trackers are placed on the user's device, except for cookies that are strictly necessary for the basic functions of the website. Moreover, a higher threshold of consent should be required for cookies used for direct marketing. Besides, it is proposed that the use of pre-ticked consent boxes, where the user must voluntarily reject non-essential cookies, should be banned. For cookie walls that blocks the user's access until the user accepts the use of cookies, they should also be prohibited. For companies that violate the consent requirement, it is also proposed that fines should be imposed to protect data privacy.

(III) Third party liability

Although DPP 2 provides that outsourced third parties must prohibit unnecessary data retention, certain data processors may not be liable under the scope of the PDPO.[20] As the data processor is not regarded a data used if he only stores and uses personal data not for his own purposes but for another person, these parties who transfer the data to another party may not be regulated under the PDPO. Similarly, this applies to website publishers, as they only facilitate the data transfer to the advertising operator. As they only provide a platform for the transfer of data, they are not caught within the PDPO.

---

[19] Information Commissioner's Office, "Guidance on the rules on use of cookies and similar technologies" Version 2 13th December 2011 at 25 & Information Commissioner's Office "Guidance on the rules on use of cookies and similar technologies" Version 3 May 2012 at 6.

[20] *Ibid* 6

Hence, it is proposed that third parties, such as outsourced data processors or website publishers, have a legal obligation to disclose the cookies that are used in websites or devices in their cookie policy. Moreover, they should inform users of any website trackers that are used.