Online Behavioural Tracking

This information leaflet aims to highlight to organisations what they should consider before deployment of online tracking on their websites. It explains the relationship between online behavioural tracking, personal data and the Personal Data (Privacy) Ordinance ("the Ordinance").

What is Online Tracking?

Website operators/owners often collect information regarding their users' online interaction with the websites. Information such as user's identity, display and/or language preference, web pages visited, items purchased, and transactions performed may be collected and recorded.

The purposes of collecting such information vary and may include:

• remembering a user's preference (e.g. on language, font size, colour scheme) so that the look and feel of a website is kept for a user upon his/her subsequent visits;
• analysing how users navigate a website with a view to optimising its design;
• establishing and maintaining a user's logged-on identity so that he/she can move around the website without being asked to log on again; or
• tracking the behaviour and preferences of an online user with a view to building detailed profiles of the user for serving marketing information or advertisements to him/her.

It is this last category of online behavioural tracking that has aroused public concerns. Online behavioural advertisers often use sophisticated algorithms to analyse the collected data, build detailed profiles of the website users, and categorise them accordingly. The user categories are then targeted by the website operators/owners or a third party for the presentation of marketing material or advertisements considered to be relevant to them.

Recommended practices on using cookies

Where cookies are used to collect behavioural information, the following additional best practices are recommended:

(a) To provide an easy-to-use way to log out of the service;
(b) To set a reasonable expiry date for cookies;
(c) To encrypt the content of cookies wherever appropriate; and
(d) To set a reasonable expiry date for cookies unless the information collected is required for the purpose of maintaining the security of the website.

Recommended practices for non advertising/marketing related tracking

3. Even if organisations are not carrying out such online tracking for advertising/marketing purposes, they should also consider adopting the best practices in items 2(a) to 2(f) above that are applicable in their circumstances.

Office of the Privacy Commissioner for Personal Data, Hong Kong
Enquiry Hotline : (852) 2827 2827
Fax : (852) 2877 7026
Address : 12/F, 248 Queen’s Road East, Wanchai, Hong Kong
Website : www.pcpd.org.hk
Email : enquiry@pcpd.org.hk

Copyrights
Reproduction of all or any parts of this information leaflet is permitted on condition that it is for non-profit making purposes and an acknowledgement of this work is duly made in reproduction.

Disclaimer
The information provided in this information leaflet is for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance (the Ordinance). For a complete and definitive statement of law, direct reference should be made to the Ordinance itself. The Commissioner makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the above information. The above suggestions will not affect the functions and powers conferred upon the Commissioner under the Ordinance.

© Office of the Privacy Commissioner for Personal Data, Hong Kong
First published in July 2012
April 2014 (First Revision)

(c) Flash/cookie/super cookies are cookies that ignore the browser’s setting on whether to accept cookies and store themselves in users’ devices (Flash cookies), or are stored in obscure places and/or would recreate themselves by various ‘secret’ techniques even if they are deleted by users (cookies/super cookies).

(d) To pre-set a reasonable expiry date for cookies;
(e) To encrypt the contents of cookies wherever appropriate; and
(f) Not to deploy techniques such as Flash/cookie/super cookies that ignore browser settings on cookies unless organisations can offer an option to website users to disable or reject such cookies.

Online Behavioural Tracking

This information leaflet aims to highlight to organisations what they should consider before deployment of online tracking on their websites. It explains the relationship between online behavioural tracking, personal data and the Personal Data (Privacy) Ordinance ("the Ordinance").

What is Online Tracking?

Website operators/owners often collect information regarding their users’ online interaction with the websites. Information such as user’s identity, display and/or language preference, web pages visited, items purchased, and transactions performed may be collected and recorded.

The purposes of collecting such information vary and may include:

• remembering a user’s preference (e.g. on language, font size, colour scheme) so that the look and feel of a website is kept for a user upon his/her subsequent visits;
• analysing how users navigate a website with a view to optimising its design;
• establishing and maintaining a user’s logged-on identity so that he/she can move around the website without being asked to log on again; or
• tracking the behaviour and preferences of an online user with a view to building detailed profiles of the user for serving marketing information or advertisements to him/her.

It is this last category of online behavioural tracking that has aroused public concerns. Online behavioural advertisers often use sophisticated algorithms to analyse the collected data, build detailed profiles of the website users, and categorise them accordingly. The user categories are then targeted by the website operators/owners or a third party for the presentation of marketing material or advertisements considered to be relevant to them.

Recommended practices on using cookies

Where cookies are used to collect behavioural information, the following additional best practices are recommended:

(a) To provide an easy-to-use way to log out of the service;
(b) To set a reasonable expiry date for cookies;
(c) To encrypt the content of cookies wherever appropriate; and
(d) To set a reasonable expiry date for cookies unless the information collected is required for the purpose of maintaining the security of the website.

Recommended practices for non advertising/marketing related tracking

3. Even if organisations are not carrying out such online tracking for advertising/marketing purposes, they should also consider adopting the best practices in items 2(a) to 2(f) above that are applicable in their circumstances.

Office of the Privacy Commissioner for Personal Data, Hong Kong
Enquiry Hotline : (852) 2827 2827
Fax : (852) 2877 7026
Address : 12/F, 248 Queen’s Road East, Wanchai, Hong Kong
Website : www.pcpd.org.hk
Email : enquiry@pcpd.org.hk

Copyrights
Reproduction of all or any parts of this information leaflet is permitted on condition that it is for non-profit making purposes and an acknowledgement of this work is duly made in reproduction.

Disclaimer
The information provided in this information leaflet is for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance (the Ordinance). For a complete and definitive statement of law, direct reference should be made to the Ordinance itself. The Commissioner makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the above information. The above suggestions will not affect the functions and powers conferred upon the Commissioner under the Ordinance.

© Office of the Privacy Commissioner for Personal Data, Hong Kong
First published in July 2012
April 2014 (First Revision)

Flash/cookie/super cookies are cookies that ignore the browser's setting on whether to accept cookies and store themselves in users’ devices (Flash cookies), or are stored in obscure places and/or would recreate themselves by various ‘secret’ techniques even if they are deleted by users (cookies/super cookies).

(c) To respect users' wish not to be tracked or to offer users a way to opt out of the tracking, especially if this is conducted by third-parties and inform them of the consequence of opting out. It is not possible to opt out of tracking while using the website, explain why this is not possible so that website users can decide whether to continue using the website.

The above measures should be carried out in a user-friendly manner ensuring that they are easily accessible and comprehensible to the website users, including teenagers/children.

Recommended practices on using cookies

(a) To pre-set a reasonable expiry date for cookies;
(b) To encrypt the contents of cookies whenever appropriate; and
(c) Not to deploy techniques such as Flash/cookie/super cookies that ignore browser settings on cookies unless organisations can offer an option to website users to disable or reject such cookies.

Recommended practices for non advertising/marketing related tracking

3. Even if organisations are not carrying out such online tracking for advertising/marketing purposes, they should also consider adopting the best practices in items 2(a) to 2(f) above that are applicable in their circumstances.

Office of the Privacy Commissioner for Personal Data, Hong Kong
Enquiry Hotline : (852) 2827 2827
Fax : (852) 2877 7026
Address : 12/F, 248 Queen’s Road East, Wanchai, Hong Kong
Website : www.pcpd.org.hk
Email : enquiry@pcpd.org.hk

Copyrights
Reproduction of all or any parts of this information leaflet is permitted on condition that it is for non-profit making purposes and an acknowledgement of this work is duly made in reproduction.

Disclaimer
The information provided in this information leaflet is for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance (the Ordinance). For a complete and definitive statement of law, direct reference should be made to the Ordinance itself. The Commissioner makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the above information. The above suggestions will not affect the functions and powers conferred upon the Commissioner under the Ordinance.

© Office of the Privacy Commissioner for Personal Data, Hong Kong
First published in July 2012
April 2014 (First Revision)

Flash/cookie/super cookies are cookies that ignore the browser’s setting on whether to accept cookies and store themselves in users’ devices (Flash cookies), or are stored in obscure places and/or would recreate themselves by various ‘secret’ techniques even if they are deleted by users (cookies/super cookies).
Online Behavioural Tracking, Personal Data and the Ordinance

Whether behavioural information collected constitutes personal data must be judged on a case by case basis. It depends on whether the information satisfies all of the three conditions below:
(a) relating directly or indirectly to a living individual;
(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
(c) in a form in which access to or processing of the information is practicable.

If it is reasonably practicable to ascertain the identity of the individual directly or indirectly from the behavioural tracking information collected (for instance, the information contains a unique identifier e.g. an account name or number), then such information would most likely be regarded as “personal data” under the Ordinance.

In other cases where the information collected does not contain unique identifiers, organisations must carefully assess if such information taken in its totality can be used to directly or indirectly identify an individual. Organisations should be in a position to ask themselves if they collect a complete set of such identifiers which, when combined together, may themselves be sufficient to ascertain the identity of an individual.

What Organisations Should Do

Following requirements under the Ordinance when personal data is involved:

1. If organisations deploy online tracking on their websites which involve the collection of “personal data” of website users, they must observe the requirements under the Ordinance including the six Data Protection Principles (“DPPs”) regarding the collection, holding and use of personal data. Specifically, such data users must ensure that the following requirements are met:
   (a) Purpose and Manner of Collection
      Online tracking must be conducted in a lawful and fair manner. The purposes of online tracking must be related to a function or activity of the data user. Information collected must be adequate but not excessive. A Personal Information Collection Statement outlined under DPP(3) must be provided to data subjects;
   (b) Accuracy and Duration of Retention
      Online tracking information held by data users should be accurate and should not be kept longer than necessary;
   (c) Use of Personal Data
      Online tracking information can only be used for the original purposes stated at the time of collection. Data users must obtain data subjects’ express and voluntary consent for any change to the purpose of use;

2. In case organisations are uncertain as regards whether the behavioural information they collected for advertising/marketing purposes would constitute “personal data”, they are strongly advised to adopt fair and transparent practices outlined below in order to promote consumer trust in their online activities.
   (a) To inform users what types of information are being collected by tracking them, the purposes of collecting the information, how the information is collected (including what tools are used), whether the information would be transferred to other parties and for how long the information will be kept.
   (b) To inform users whether any third-party is collecting or tracking their behavioural information. As the organisation is the entity which engages the third-party to collect or track user behaviour, it is the organisation’s responsibility to enable users to understand what third-party information is being collected by the organisation and how the means by which the information is collected. Organisations should inform users of the nature of such third-parties, purposes and means of collection, retention period and whether such information collected would be further transferred to other parties by the third party.
Means of Online Tracking

There are a number of means by which organisations may track and record the online behaviour of website users. It is important to note that this information is typically used to track the user's online activity on websites, as well as their browsing habits on different websites.

The following are some common means of tracking:

- At the webserver end, by recording and retaining an authenticated user's dealings and behaviour on the website, such as information searched, transactions conducted, and browser purchasing history;
- At the webserver end, by using techniques such as placing web beacons or web bugs on webpages;
- At the user-end, by downloading cookies³ or files or programmes from websites to browser devices, and having the user's browsing behaviour towards the websites recorded in these downloaded files/programmes.

It is worth noting that, by deploying techniques such as third-party cookies⁴ or web bugs, a third-party website which a user has not directly accessed can still track the user's behaviour.

Concerns with Online Behavioural Tracking

Online behavioural tracking may be a concern for website users because of the following reasons:

- Website users' information or browsing habits are often collected by the website operator/owner without their knowledge or consent.
- The collected information does not contain unique identifiers, which enables organisations to build a profile of the user, without their knowledge or consent.
- The information collected may be combined with information collected from other websites or sources about that user, thus building his/her profile without his/her knowledge.
- Website users are not offered the option to opt out of the use of tracking information.
- Information about a website user collected from one website may be combined with information collected from other websites or sources about that user.

What Organisations Should Do

Following requirements under the Ordinance when personal data is involved

1. If organisations deploy online tracking on their websites which involve the collection of “personal data” of website users, they must observe the requirements under the Ordinance including the six Data Protection Principles ("DPPs") regarding the collection, holding and use of the personal data. Specifically, such data users must ensure that the following requirements are met:

- (a) To inform users what types of information are being collected or tracked by them, the purpose of collecting this data, and that website users are not offered the option to opt out of the use of tracking information.
- (b) Website users' information or browsing habits may even be collected by a third party without website users' knowledge or consent.
- (c) The collected information may be transferred to other parties by the website operator/owners or the third party without website users' knowledge or consent.
- (d) Information about a website user collected from one website may be combined with information collected from other websites or sources about that user, thus building his/her profile without his/her knowledge.
- (e) The purpose of collecting the information is not made clear to the website users. Even if this has been made clear, website users are not offered the option to opt out of the use.

Online Behavioural Tracking, Personal Data and the Ordinance

Whether behavioural information collected constitutes personal data must be judged on a case by case basis. It depends on whether the information satisfies all of the three conditions below:

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

If it is reasonably practicable to ascertain the identity of the individual directly or indirectly from the behavioural tracking information collected, the information contains a unique identifier e.g. an account name or number, then such information would most likely be regarded as “personal data” under the Ordinance.

In other cases where the information collected does not contain unique identifiers, organisations must carefully assess if such information taken in its totality can be used directly or indirectly to identify an individual. Organisations should also bear in mind that when they collect a complex set of such identifiers which, when combined together, may themselves be sufficient to ascertain the identity of an individual.

What Should Organisations Do

1. If organisations deploy online tracking on their websites which involve the collection of “personal data” of website users, they must observe the requirements under the Ordinance including the six Data Protection Principles ("DPPs") regarding the collection, holding and use of the personal data. Specifically, such data users must ensure that the following requirements are met:

- (a) Purpose and Manner of Collection
- (b) Accuracy and Duration of Retention
- (c) Use of Personal Data

2. In case organisations are uncertain as regards whether the behavioural information they collected for advertising/ marketing purposes would constitute “personal data”, they are strongly advised to adopt fair and transparent practices outlined below in order to promote consumer trust in their online activities.

- (a) To inform users what types of information are being collected by third-party cookies from them, the purpose of collecting this information, the means by which the information is collected (including what tools are used), whether the information will be transferred to third-parties and if so, the classes of such third-parties and purpose of transfer, whether the information will be integrated with other information to track identifiable users and for how long the information will be kept.
- (b) To inform users whether any third party is collecting or tracking their behavioural information. As the organisation is the entity which engages the third-party to collect or track user behaviour, it is the organisation’s responsibility to understand whether the third-party what information is being collected, the means by which the information is collected, Organisations should inform users of the nature of such third parties, purposes and means of collection, retention period and whether such information collected would be further transferred to other parties by the third party.

Recommended practice on fair and transparency when there is uncertainty

1. In case organisations are uncertain as regards whether the behavioural information they collected for advertising/ marketing purposes would constitute “personal data”, they are strongly advised to adopt fair and transparent practices outlined below in order to promote consumer trust in their online activities.

- (a) To inform users what types of information are being collected by third-party cookies from them, the purpose of collecting this information, the means by which the information is collected (including what tools are used), whether the information will be transferred to third-parties and if so, the classes of such third-parties and purpose of transfer, whether the information will be integrated with other information to track identifiable users and for how long the information will be kept.
- (b) To inform users whether any third party is collecting or tracking their behavioural information. As the organisation is the entity which engages the third-party to collect or track user behaviour, it is the organisation’s responsibility to understand whether the third-party what information is being collected, the means by which the information is collected, Organisations should inform users of the nature of such third parties, purposes and means of collection, retention period and whether such information collected would be further transferred to other parties by the third party.

---

³ Available at: www.privacy.gov.hk/english/onlineprivacy/guidance.html


Means of Online Tracking

There are a number of means by which organisations may track and record the online behaviour of website users. It is important to note that this information leaflet applies to online tracking in general and is not limited to any specific means of online tracking. While the following examples are some common tools of tracking, rapid developments in online technology mean that other tools may be developed that would serve the same purpose.

(a) At the webserver end, by recording and retaining an authenticated user’s dealings and behaviour on the website, such as information searched, transactions conducted, and his/her purchasing history; and
(b) At the webserver end, by using techniques such as placing web beacons or bugs on webpage(s) and/or
(c) At the user-end, by downloading cookies1, files or programmes from websites to browser devices, and having the user’s browsing behaviour towards the website recorded in these downloaded files/programmes.

It is worth noting that, by deploying techniques such as third-party cookies1 or web bugs2, a third-party website which a user has not directly accessed can still track the user’s behaviour.

Concerns with Online Behavioural Tracking

Online behavioural tracking may be a concern for website users because of the following main reasons:

(a) Website users’ information or browsing habits are often collected by the website operator/owner without website users’ knowledge or consent; and
(b) Website users’ information or browsing habits may even be collected by a third party without website users’ knowledge or consent.

The collected information may be transferred to other parties by the website operators/owners or the third parties from which the information is collected. When web bug links to the same central server are placed in multiple websites, all users visiting these websites will have their online behaviour collated by the central server.

Online Behavioural Tracking, Personal Data and the Ordinance

Whether behavioural information collected constitutes personal data must be judged on a case-by-case basis. It depends on whether the information satisfies all of the three conditions below:-

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

It is reasonably practicable to ascertain the identity of the individual directly or indirectly from the behavioural tracking information collected (for instance, the information contains a unique identifier e.g., an “anonymous” name or number), then such information would most likely be regarded as “personal data” under the Ordinance.

In other cases where the information collected does not contain unique identifiers, organisations must carefully assess if such information taken in its totality can be used to directly or indirectly identify an individual. Organisations should bear in mind that when they collect a complex set of such identifiers which, when combined together, may themselves be sufficient to ascertain the identity of an individual.

What Organisations Should Do

Following requirements under the Ordinance when personal data is involved

1. If organisations deploy online tracking on their websites which involve the collection of “personal data” of website users, they must observe the requirements under the Ordinance including the six Data Protection Principles (“DPPs”) regarding the collection, holding and use of the personal data. Specifically, such data users must ensure that the following requirements are met:

(a) Purpose and Manner of Collection

Online tracking must be conducted in a lawful and fair manner. The purpose(s) of online tracking must be related to a function or activity of the data user. Information collected must be adequate but not excessive. A Personal Information Collection Statement outlined under DPP9 must be provided to data subjects;

(b) Accuracy and Duration of Retention

Online tracking information held by data users should be accurate and should not be kept longer than necessary;

(c) Use of Personal Data

Online tracking information can only be used for the original purposes stated at the time of collection. Data users must obtain data subjects’ express and voluntary consent for any change to the purpose of use;

2. In case organisations are uncertain as regards whether the behavioural information they collected for advertising/marketing purposes would constitute “personal data”, they are strongly advised to adopt fair and transparent practices outlined below in order to promote consumer trust in their online activities.

(a) To inform users what types of information are being collected and track them, the purposes of collecting the information, how the information is collected (including what tools are used), whether the information would be transferred to third-parties (and if so, the classes of such third-parties and purpose of transfer), whether the information will be kept, and whether the information would be combined with other information to track individual users and for how long the information will be kept.

(b) To inform users whether any third party is collecting or tracking their behavioural information. As the organisation is the entity which engages the third party to collect or track user behaviour, it is the organisation’s responsibility to understand and inform the third party what information is being collected, how it is collected, how it will be used, and the means by which the information is collected. Organisations should inform users of the nature of such third parties, purposes and means of collection, retention period and whether such information collected would be further transferred to other parties by the third party.

Recommended practice on fair and transparency when there is uncertainty

1. website users are not offered the option to opt out of the use.


The above measures should be carried out in a user-friendly manner ensuring that they are easily accessible and comprehensible to the website users, including teenagers/children.

**Recommended practices on using cookies**

Where cookies are used to collect behavioural information, the following additional best practices are recommended:

(a) To set a reasonable expiry date for cookies;
(b) To encrypt the contents of cookies whenever appropriate; and
(c) Not to deploy techniques such as Flash/cookie super cookies* that ignore browser settings on cookies unless organisations can offer an option to website users to disable or reject such cookies.

**Recommended practices for non advertising/marketing related tracking**

3. Even if organisations are not carrying out such online tracking for advertising/marketing purposes, they should also consider adopting the best practices in items 2(a) to 2(f) above that are applicable in their circumstances.

---

*Flash/cookie super cookies are cookies that ignore the browsers’ setting on whether to accept cookies and store themselves in users’ devices (Flash cookies), or are stored in obscure places and/or would recreate themselves by various ‘secret’ techniques even if they are deleted by users (cookie super cookies).

---

**What is Online Tracking?**

Website operators/owners often collect information regarding their users’ online interaction with their websites. Information such as user’s identity, display and/or language preference, web pages visited, items purchased, and transactions performed may be collected and recorded.

The purposes of collecting such information vary and may include:

- remembering a user’s preference (e.g. on language, font size, colour scheme) so that the look and feel of a website is kept for a user upon his/her subsequent visits;
- analysing how users navigate a website with a view to optimising its design;
- establishing and maintaining a user’s logged-on identity so that he/she can move around the website without being asked to log on again; or
- tracking the behaviour and preferences of an online user with a view to building detailed profiles of the user for serving marketing information or advertisements to him/her.

It is this last category of online behavioural tracking that has aroused public concerns. Online behavioural advertisers often use sophisticated algorithms to analyse the collected data, build detailed profiles of the website users, and categorise them accordingly. The user categories are then targeted by the website operators/owners or a third party for the presentation of marketing material or advertisements believed to be relevant to them.

**Recommended practices for non advertising/marketing related tracking**

3. Even if organisations are not carrying out such online tracking for advertising/marketing purposes, they should also consider adopting the best practices in items 2(a) to 2(f) above that are applicable in their circumstances.

---

**Recommended practices on using cookies**

Where cookies are used to collect behavioural information, the following additional best practices are recommended:

(a) To set a reasonable expiry date for cookies;
(b) To encrypt the contents of cookies whenever appropriate; and
(c) Not to deploy techniques such as Flash/cookie super cookies* that ignore browser settings on cookies unless organisations can offer an option to website users to disable or reject such cookies.

---

**Recommended practices for non advertising/marketing related tracking**

3. Even if organisations are not carrying out such online tracking for advertising/marketing purposes, they should also consider adopting the best practices in items 2(a) to 2(f) above that are applicable in their circumstances.

---

**What is Online Tracking?**

Website operators/owners often collect information regarding their users’ online interaction with the websites. Information such as user’s identity, display and/or language preference, web pages visited, items purchased, and transactions performed may be collected and recorded.

The purposes of collecting such information vary and may include:

- remembering a user’s preference (e.g. on language, font size, colour scheme) so that the look and feel of a website is kept for a user upon his/her subsequent visits;
- analysing how users navigate a website with a view to optimising its design;
- establishing and maintaining a user’s logged-on identity so that he/she can move around the website without being asked to log on again; or
- tracking the behaviour and preferences of an online user with a view to building detailed profiles of the user for serving marketing information or advertisements to him/her.

It is this last category of online behavioural tracking that has aroused public concerns. Online behavioural advertisers often use sophisticated algorithms to analyse the collected data, build detailed profiles of the website users, and categorise them accordingly. The user categories are then targeted by the website operators/owners or a third party for the presentation of marketing material or advertisements considered to be relevant to them.
This information leaflet aims to highlight to organisations what they should consider before deployment of online tracking on their websites. It explains the relationship between online behavioural tracking, personal data and the Personal Data (Privacy) Ordinance (“the Ordinance”).

What is Online Tracking?
Website operators/owners often collect information regarding their users’ online interaction with the websites. Information such as user’s identity, display and/or language preference, web pages visited, items purchased, and transactions performed may be collected and recorded.

The purposes of collecting such information vary and may include:
- remembering a user’s preference (e.g. on language, font size, colour scheme) so that the look and feel of a website is kept for a user upon his/her subsequent visits;
- analysing how users navigate a website with a view to optimising its design;
- establishing and maintaining a user’s logged-on identity so that he/she can move around the website without being asked to log on again; or
- tracking the behaviour and preferences of an online user with a view to building detailed profiles of the user for serving marketing information or advertisements to him/her.

It is this last category of online behavioural tracking that has aroused public concerns. Online behavioural advertisers often use sophisticated algorithms to analyse the collected data, build detailed profiles of the website users, and categorise them accordingly. The user categories are then targeted by the website operators/owners or a third party for the presentation of marketing material or advertisements considered to be relevant to them.

Recommended practices on using cookies
Where cookies are used to collect behavioural information, the following additional best practices are recommended:

- To pre-set a reasonable expiry date for cookies;
- To encrypt the contents of cookies wherever appropriate; and
- Not to deploy techniques such as Flash/cookie/super cookies\(^*\) that ignore browser settings on cookies unless organisations can offer an option to website users to disable or reject such cookies.

Recommended practices for non advertising/marketing related tracking
3. Even if organisations are not carrying out such online tracking for advertising/marketing purposes, they should also consider adopting the best practices in items 2(a) to 2(j) above that are applicable in their circumstances.

Office of the Privacy Commissioner for Personal Data, Hong Kong

Disclaimer
The information provided in this information leaflet is for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance (the Ordinance). For a complete and definitive statement of law, direct reference should be made to the Ordinance itself. The Commissioner makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the above information. The above suggestions will not affect the functions and powers conferred upon the Commissioner under the Ordinance.

\(^*\) Flash/cookie/super cookies are cookies that ignore the browsers’ setting on whether to accept cookies and store themselves in users’ devices (Flash cookies), or are stored in obscure places and/or would recreate themselves by various ‘social’ techniques even if they are deleted by users (cookie/super cookies).

© Office of the Privacy Commissioner for Personal Data, Hong Kong
First published in July 2012
April 2014 (First Revision)

Enquiry Hotline : (852) 2827 2827
Fax : (852) 2877 7026
Address : 12/F, 248 Queen’s Road East, Wanchai, Hong Kong
Website : www.pcpd.org.hk
Email : enquiry@pcpd.org.hk

Copyrights
Reproduction of all or any parts of this information leaflet is permitted on condition that it is for non-profit making purposes and an acknowledgement of this work is duly made in reproduction.

First published in July 2012
April 2014 (First Revision)