Prime Minister's Office
Data Protection Office

Data Protection -
Online Behavioural Advertising, Search Engines and Social Networking Sites: What is the connection?

Volume 8

Data Protection -

Online Behavioural Advertising, Search Engines and Social Networking Sites:

What is the connection?

Volume 8

Data Protection Commissioner
(Mrs Drudeisha Madhub)

TABLE OF CONTENTS

INTRODUCTION

The connection between these intertwined concepts - online behavioural advertising, social networking sites and search engines, has given rise to major concerns both locally and internationally with regard to the potential and concrete risks entailed to the right to privacy and protection of personal data of all internet users or to use a strong expression, the addicts of the virtual world.

This guide will try to explain these 3 concepts from a data protection perspective for a judicious and cautious use of these facilities in the future and is targeted to those data controllers, processors and subjects using them. This guide further contains technical material which may not be easily understandable but which has however been simplified for the benefit of all readers. The Commissioner would like to emphasize that this guide should be read in conjunction with the other guidelines produced by this office, namely volumes 1, 2 and 4 for any training to be successful as they are complementary and explain all the underlying concepts in the Data Protection Act.

Internet service providers as data controllers and/or processors, are under many obligations under the Data Protection Act (DPA) including namely the eight principles contained in the First Schedule to the Act which are the eight commandments of Data Protection:-

Data Protection Principles

First principle

Personal data shall be processed fairly and lawfully.

Second principle

Personal data shall be obtained only for any specified and lawful purpose, and shall not be further processed in any manner incompatible with that purpose.

Third principle

Personal data shall be adequate, relevant and not excessive in relation to the purpose for which they are processed.

Fourth principle

Personal data shall be accurate and, where necessary, kept up to date.

Fifth principle

Personal data processed for any purpose shall not be kept longer than is necessary for that purpose or those purposes.

Sixth principle

Personal data shall be processed in accordance with the rights of the data subjects under this Act.

Seventh principle

Appropriate security and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Eighth principle

Personal data shall not be transferred to another country, unless that country ensures an adequate level of protection for the rights of data subjects in relation to the processing of personal data.

Part IV of the Act establishes the obligations to collect personal data in a responsible way by imposing through section 22, the duty to inform the user/s of the identity of the data controller, the purposes for which the data are being collected, the intended recipients or beneficiaries of the data, whether the express consent of the user/s is/are required for the collection and the right of the user/s to access the data, amongst others. Section 27 further unfolds the duty of the data controller to cater for appropriate security and organisational measures in order to protect the processing or collection of the data.

The World Wide Web currently thrives on privacy invading technologies which carry out processing operations of personal data invisible to the data subject. In other words, the Internet user is not aware that his/her personal data have been collected and further processed, and might be used for purposes unknown to him/her. The data subject either enjoys no or limited freedom of choice as regards the use of his personal data.

One example is the so-called **cookie**, which can be defined as a computer record of information that is sent from a web server to a user's computer for the purpose of future identification of that computer on subsequent visits to the same website. The cookie is a short alphanumeric text which is stored (and later retrieved) on the data subject's terminal equipment by a network provider.

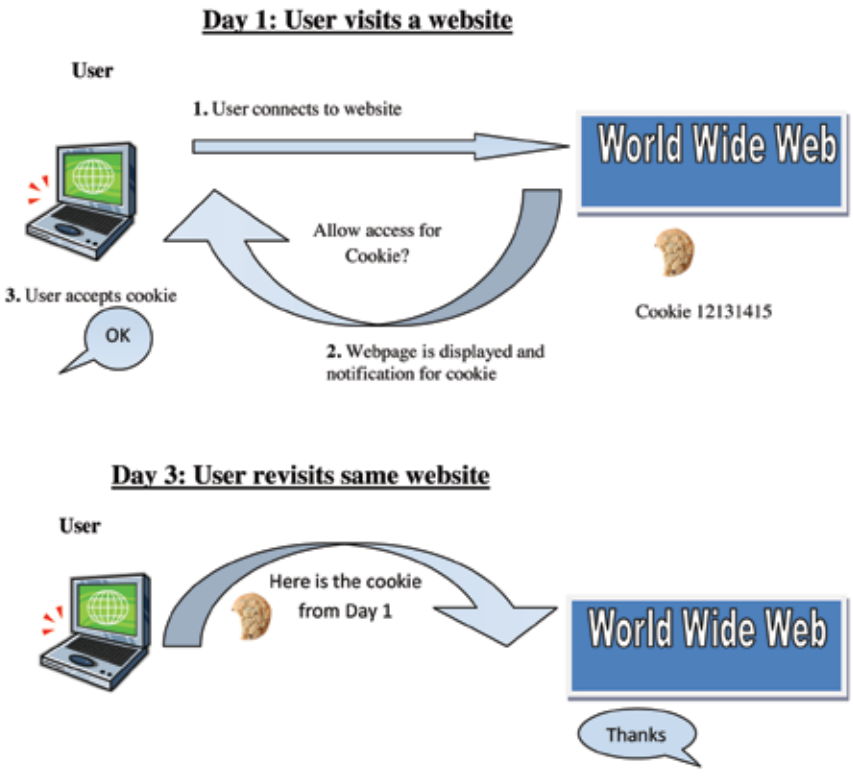

Fig 1: Connecting to the World Wide Web with cookies

The user should be informed when a cookie is intended to be received, stored or sent by the Internet Software. The message should specify, in clear terms, which personal information is intended to be stored in the cookie, for what purpose as well as the period of validity of the cookie.

Example of a notification message for a cookie:

Purpose: Our website uses cookies for user authentication in order to respond faster to your web queries

Cookie name: A (optional) Accept Reject
Content: personal info to register an account
Expiry: 1 year/ when de-registering from the service

Thus, the first time a user comes in contact with the service provider (through a website visit), no cookie has been set, and no cookie will be sent to him. The provider can display a message in any type of information area (including the area where the product would appear) to propose a choice to the user:

- Accept an "opt-in" cookie for the purpose of future behavioural advertising for example.
- Reject cookies for the purpose of behavioural advertising whilst at the same time accepting a cookie containing the word "REJECT" so that this refusal can be recorded.
- Store no cookie at all. In that case, the user will be asked again about his choice during the next visit.

Another example is "**Browsers**" which are software programs designed to, amongst other things, graphically display material that is available on the Internet. Browsers communicate between the user's computer and the remote computer where information is stored, i.e, the Web server. Browsers often send more information to the Web server than strictly necessary for establishing the communication. Classical browsers will automatically send to the Webserver visited the type and language of the browser, the name of other software programs installed on the user's PC and operating system, the referring page, cookies etc. Such data can also be transmitted systematically to third parties by the browser software, in an invisible way.

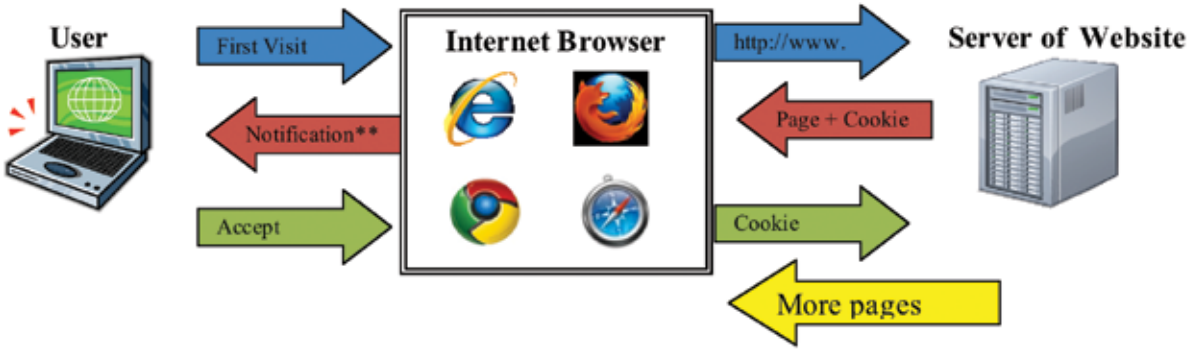

Fig 2: Connecting to the World Wide Web with browser

On establishing a connection with a web server (sending a request or receiving a Web page), the user must be informed which information is intended to be transferred and for what purposes. Hyperlinks are also sent by a website to a user, and the user's browser should be able to reveal them all to the user.

Example of a notification message for a browser:

Purpose: Our website uses cookies for user tracking in order to understand site preferences and improve content and design of website

Cookie name: abc (optional) Accept Reject
Content: the pages visited by the user during the visit
Expiry: when user exits the browser

These techniques allow the creation of click trails about the Internet user. Click trails consist of information about an individual's behaviour, identity, pathway or choices expressed while visiting a web site. They contain the links that a user has followed and are logged in the web server.

Being given that not all users share the same level of IT literacy, internet hardware and software developers and designers should ensure that the users are given adequate opportunity to understand all the implications of the use of their personal data. The configuration of hardware and software products should not, by default, allow for collecting, storing or sending of client persistent or recurrent information. For example: Browser software should, by default, be configured in such a way that only the minimum amount of information necessary for establishing an Internet connection is processed. Cookies should, by default, not be sent or stored.

During its installation, a browser's feature designed to store and send data about a user's identity or profile should not be filled in automatically with any data previously stored on the user's equipment.

Internet hardware and software products should allow the data subject to freely decide about the processing of his/her personal data by offering user-friendly tools to filter (i.e. to reject or to modify) the reception, storage or sending of client persistent information following certain criteria (including profiles, the domain or the identity of the Internet server, the kind and the duration of the information being collected, stored or sent and so on).

The user should be provided with clear instructions regarding the use of software and hardware for the implementation of these options and tools. For example: browser software should provide options so that the user can configure the browser, specifying which information the browser should or should not collect and transmit.

This means for cookies that the user should always be given the option to accept or reject the sending or storage of a cookie as a whole. Also the user should be given options to determine which pieces of information should be kept or removed from a cookie, depending on e.g. the period of validity of the cookie or the sending and receiving Web sites. Internet software and hardware products should allow the users to remove client persistent information in a simple way and without involving the sender. The user should be given clear instructions on how to do this. If the information cannot be removed, there must be a reliable way to prevent it from being transferred and read. Cookies and other client persistent information should be stored in a standardised way and be easily and selectively erasable at the client's computer.

ONLINE BEHAVIOURAL ADVERTISING

Fig 3: Online Behavioural Advertising

Undeniably, online advertising is a vital source of income for a wide range of online services and is an important catalyst in the growth and expansion of the internet economy. However, the particular practice of behavioural advertising also raises important data protection and privacy related concerns.

The Data Protection Act 2004 is applicable when behavioural advertising is based on the use of identifiers that enable the creation of very detailed user profiles which, in most cases, are personal data.

Basic internet technology allows advertising network providers to track data subjects across different websites and over time. Such profiles can be used to provide data subjects with tailored advertising.

Behavioural advertising involves the following actors:

- Advertising network providers (also referred to as "ad network providers"), the most important distributors of behavioural advertising since they connect publishers with advertisers;
- Advertisers who want to promote a product or service to a specific audience; and
- Publishers who are the website owners looking for revenues by selling space to display ads on their website(s).

Usually, the publisher reserves visual space on its website to display an ad and relays the rest of the advertising process to one or more advertising network providers. The ad network provider is responsible for distributing advertisements to appropriate publishers.

Applicability of DPA, Obligations and Rights

Providing highly visible information is a precondition for consent to be valid. Mentioning the practice of behavioural advertising in general terms and conditions and/or privacy policies can never suffice. Notices provided in general terms and conditions and/or privacy policies, often drafted in rather obscure ways fall short of the requirements of the Data Protection Act.

In this regard and taking into account the average low level of knowledge about the practice of behavioural advertising, efforts should be applied to change this situation. In practical terms, data controllers should ensure that individuals are told, at a minimum, who (i.e. which entity) is responsible for serving the cookie and collecting the related information. In addition, they should be informed in simple ways:

- that the cookie will be used to create profiles;
- what type of information is required to be collected to build such profiles;
- that the profiles will be used to deliver targeted advertising, and,
- that the cookie will enable the user's identification across multiple web sites.

For instance in some websites, you may find the following sentence, "the *cookie stores some basic, non-personal information on your PC to improve certain functionalities and customize the surfing experience".* Behavioural advertising involves the processing of unique identifiers that are achieved through the use of cookies, or any kind of device fingerprinting. The use of such unique identifiers allows for the tracking of users of a specific computer even when IP addresses are deleted or anonymised. In other words, such unique identifiers enable data subjects to be "singled out" for the purpose of tracking user behaviour while browsing on different websites and thus qualify as personal data.

Specific software applications (browser plug-ins or extensions) could be developed by ad networks and downloaded and installed by users to enable changing the status of browser settings with regard to advertising-related cookies by means of application programming interfaces (API) or other tools made available by browser manufacturers. Users should receive the relevant information on data processing as a preliminary step to installing the specific "advertising" plug-in. One might argue that a prerequisite for this opt-in mechanism to work appropriately consists in ensuring that third-party cookies are not accepted by default in browser settings.

Such a privacy solution is 'Do Not Track', a consent mechanism based on browser settings. However, such a mechanism should truly enable users to express their consent on a case by case basis, without being tracked by default.

Network providers/ publishers should provide the information directly on the screen, interactively, if needed, through layered notices and it should be easily accessible.

Icons placed on the publishers' website, around advertising, with links to additional information, are good examples. Network providers/publishers should be creative in this area.

Browsers must either alone or in combination with other means effectively convey clear, comprehensive and fully visible information about the processing. Ad network providers should encourage and work with browser manufacturers/ developers to implement privacy by design in browsers.

Cookie-based opt-out mechanisms in general are not sufficient to constitute an adequate mechanism to obtain informed and express user consent. Though, in most cases, express user's consent may also be implied if they do not opt out, this does not stand to mean that the decision not to opt out is an informed one. In practice, very few people exercise the opt-out option, not because they have made an informed decision to accept behavioural advertising, but rather because they are not aware that the processing of their personal data is taking place, and/or do not know how to exercise the opt out option.

Although the opt-out cookie prevents the further reception of personalised advertising, it does not stop the advertising network from accessing and storing information in the user's terminal. On the contrary, it has been demonstrated that an ongoing technical exchange of information between the user's terminal equipment and the advertising network is still in place after the installation of the opt-out cookie.

The user is not informed on whether or not the tracking cookie remains stored in his/her computer and for what purpose.

The installation of the opt-out cookie does not offer the possibility to manage and delete previously installed tracking cookies, whereas at the same time it creates the mistaken presumption that opting out disables the tracking of internet behaviour.

It is to be noted that express consent as provided in the Data Protection Act does not automatically relate to mandatory written consent but may also be implied and non-written.

Ad network providers should create prior opt-in mechanisms. Mechanisms to deliver informed, valid consent should require an affirmative action by the data subject indicating his/her willingness to receive cookies and the subsequent monitoring of his/her surfing behaviour for the purposes of sending him/her tailored advertising.

A users' acceptance to receive a cookie could also entail his/her acceptance for the subsequent readings of the cookie, and hence for the monitoring of his/her internet browsing. It would not be necessary to request consent for each reading of the cookie. However, to ensure that data subjects remain aware of the monitoring over time, ad network providers should:

i) limit in time the scope of the express consent;

ii) offer the possibility to easily revoke their consent to being monitored for the purposes of serving behavioural advertising and;

iii) create a symbol or other tools which should be visible in all the web sites where the monitoring takes place (the website partners of the ad network provider). This symbol would not only remind individuals of the monitoring but also help them to control whether they want to continue being monitored or wish to revoke their consent.

As an example, the following cookies would be exempted from informed consent:

- ***A secure login session cookie*. This type of cookie is designed to identify the user once he/she has logged-in to an information society service and is necessary to recognise him/her, maintaining the consistency of the communication with the server over the communication network.**
- **A *shopping basket cookie*. On a shopping website, this type of cookie is typically used to store the reference of items the user has selected by clicking on a button (e.g. "add to my shopping cart"). This cookie is thus necessary to provide an information society service explicitly requested by the user.**
- ***Security cookies*. Cookies which provide security that are essential to comply with the security requirements of the Data Protection Act for an information society service explicitly requested by the user. For example, a cookie may be used to store a unique identifier to allow the information society service to provide additional assurance in the recognition of returning users. Attempted logins from previously unseen devices could prompt for additional security questions.**

Pop up screens are not the only way to obtain consent. There are many other ways, to obtain consent. Some of these examples are:

- ***A static information banner on top of a website requesting the user's consent to set some cookies, with a hyperlink to a privacy statement with a more detailed explanation about the different controllers and the purposes of the processing.***

- *A splash screen on entering the website explaining what cookies will be set, by what parties, if the user consents.*
- *A default setting prohibiting the transfer of data to external parties, requiring a user click to indicate consent for tracking purposes.*
- *A default setting in browsers that would prevent the collection of behavioural data (Do not collect).*

Network providers should ensure compliance with the purpose limitation principle and security obligations. In addition, the ad network providers should enable individuals to exercise their rights of access and rectification and erasure. For instance, some ad network providers offer data subjects the possibility to access and modify the interest categories in which they have been classified.

Ad network providers should implement retention policies which ensure that information collected each time that a cookie is read is automatically deleted after a justified period of time necessary for the purposes of the processing.

Roles and Responsibilities of the Different Players under the DPA

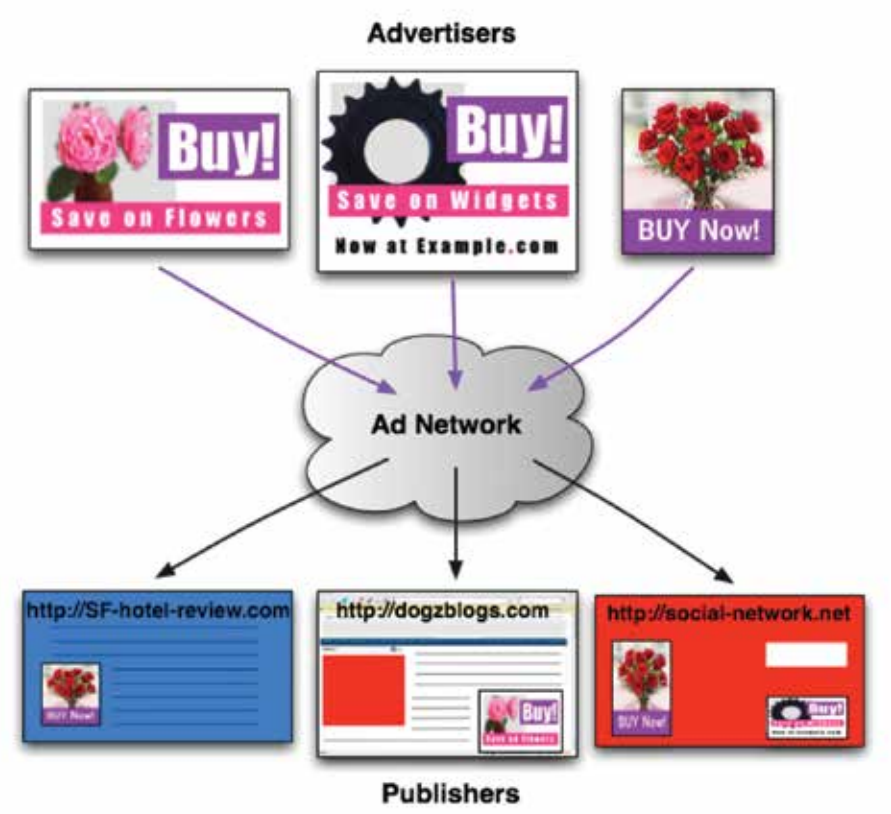

Fig 4: Example of how an ad network operates

Ad network providers are bound by the obligations of data controllers insofar as they place cookies and/or retrieve information from cookies already stored in the data subjects' terminal equipment and determine the purposes and the essential means of the processing of data. Ad network providers have complete control over the purposes and means of the processing.

They 'rent' space from publishers' web sites to place adverts and, in most cases, collect the IP address and possible other data that the browser may reveal. Further, the ad network providers use the information gathered on Internet users' surfing behaviour to build profiles and to select and deliver the ads to be displayed on the basis of this profile. In this scenario, they clearly act as data controllers, falling within the definition provided in the Data Protection Act.

Publishers, amongst others, rent out space on their websites for ad networks to place adverts. They set up their web sites in a way that visitors' browsers are automatically redirected to the webpage of the ad network provider (which will then send a cookie and serve tailored advertising). This raises the question about their responsibility vis-à-vis the data processing. Whether a publisher can be deemed to be a joint controller or a data processor with the ad network provider will depend on the conditions of collaboration between the publisher and the ad network provider.

In this regard, it is necessary to interpret the legal framework in a flexible way by applying only those provisions that are pertinent. If publishers do not hold personal information, obviously, it would not make legal sense to apply some of the obligations of the Data Protection Act.

Publishers will be joint controllers if they collect and transmit personal data regarding their visitors such as name, address, age, location, etc to the ad network provider. To the extent that publishers act as data controllers or processors, they are bound by the obligations arising under the DPA regarding the part of the data processing under their control.

In sum, publishers should be aware that by entering into contracts with ad networks with the consequence that personal data of their visitors are available to ad network providers, they take some responsibility towards their visitors. The breadth of their responsibility, including the extent to which they become data controllers or processors should be analysed on a case by case basis depending on the particular conditions of collaboration with ad network providers, as reflected in the service agreements. Accordingly, the service agreements between publishers and ad network providers should set up the roles and responsibilities of both parties in the light of their collaboration, as described in the agreement.

Publishers may also have certain data controller and processor related responsibilities regarding the processing that takes place in the first phase of the processing, i.e., when they set up their web sites, they trigger the transfer of the IP address as data controllers to ad network providers (which enable the further processing), such responsibility entails some data protection obligations. Thus, when publishers transfer

directly identifiable personal data to ad network providers themselves, they will be deemed joint controllers. Thus, even if, technically the data transfer of the IP address is carried out by the browser of the individual who visits the publisher's web site, it is not the individual who triggers the transfer.

When a data subject clicks on an ad and visits the advertisers' website, the advertiser can track which campaign resulted in the click-through. If the advertiser captures the targeting information and combines it with the data subject's onsite surfing behaviour or registration data, then the advertiser is an independent data controller for this part of the data processing.

For browser settings to be able to deliver informed consent, it should not be possible to "bypass" the choice made by the user in setting the browser. Given the importance that browser settings play in ensuring that data subjects effectively give their consent to the storage of cookies and the processing of their information, it seems of paramount importance for browsers to be provided with default privacy-protective settings, in other words, to be provided with the setting of 'non-acceptance and non-transmission of third party cookies'. To make it more effective, the browsers should require users to go through a privacy wizard when they first install or update the browser and provide for an easy way of exercising choice during use.

Children's Consent

The problems related to obtaining informed consent are further emphasised as far as children are concerned. In addition to the requirements described above (and below) for consent to be valid, in some cases children's consent must be provided by their parents or other legal representatives. This means that ad network providers would need to inform parents about the collection and the use of children's information and obtain their consent before collecting and further using their information for the purposes of engaging in behavioural targeting of children.

Taking into account the vulnerability of children, the office is of the view that ad network providers should not offer interest categories intended to serve behavioural advertising or influence children.

Obligations regarding sensitive data

Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life or data related to criminal proceedings are considered sensitive. There are serious risks to the infringement of the personal data of individuals if this type of

information is used for the purposes of serving behavioural advertising. Any possible targeting of data subjects based on sensitive information opens the possibility of abuse. Furthermore, given the sensitivity of such information and the possible awkward situations which may arise if individuals receive advertising that reveals, for example, sexual preferences or political activity, offering interest categories that would reveal sensitive data should be discouraged.

Publishers may also be liable under general principles of civil law as well as consumer protection laws related to business-to-consumer commercial practices to inform individuals insofar as the data processing and monitoring takes place as a result of their action to re-direct them to the ad network provider.

However, if nevertheless, ad network providers offer and use interest categories that reveal sensitive information, they must comply with data protection principles. For example, if an ad network provider processes individual behaviour in order to 'place him/her' in an interest category indicating a particular sexual preference, they would be processing sensitive data under section 25 of the Data Protection Act. This article prohibits the processing of sensitive data except in certain specific circumstances.

If ad network providers want to use information gathered for behavioural advertisement for secondary, incompatible purposes, for example across services, they need additional legal grounds to do so. For example, they will need to inform data subjects and, in most cases, obtain their express consent.

Compliance with the retention principle requires limiting the storage of information. Accordingly, companies must specify and respect timeframes under which data will be retained.

Pursuant to the above, information about users' behaviour has to be eliminated if it is no longer needed for the development of a profile. Indefinite or overly long retention periods contradict the Data Protection Act. Retention periods of major ad network providers may vary, with some companies using an indefinite period and others limiting the retention periods to a determined period.

Accordingly, ad network providers should implement policies to ensure that information collected each time a cookie is read, is immediately deleted or anonymised once the necessity for retaining it has expired. Each data controller needs to be able to justify the necessity for a given retention period. Ad network providers should provide reasons that justify the conservation period that they consider necessary in the light of the purposes sought by the data processing.

If/when an individual asks for a deletion of his/her profile or if he/she exercises his/her right to withdraw the consent, these actions require the ad network provider to erase or delete promptly the data subject's information in so far as the ad network provider ceases to have the necessary legal grounds allowing the processing.

SOCIAL NETWORKING SITES (SNS)

The evolution of web communities and hosted services such as social network services ("SNS") is a relatively recent phenomenon, with the number of users multiplying at an incredibly exponential rate.

SNS can broadly be defined as online communication platforms which enable individuals to join or create networks of like-minded users. SNS share certain characteristics:

- Users are invited to provide personal data for the purpose of generating a description of themselves or 'profile'.
- SNS also provide tools which allow users to post their own material (user-generated content such as a photograph or a diary entry, music or video clip or links to other sites).
- 'Social networking' is enabled using tools which provide a list of contacts for each user, and with which users can interact.

SNS generate much of their revenue through advertising which is served alongside the webpages set up and accessed by users. Users who post large amounts of information about their interests on their profiles offer a refined market to advertisers wishing to serve targeted advertisements based on that information.

It is therefore important that SNS as data controllers operate in a way which respects the rights and freedoms of users (data subjects) who have a legitimate expectation that the personal data they disclose will be processed in accordance with data protection principles. Secure processing of information is a key element of trust in SNS. Controllers must take the appropriate technical and organisational measures, both at the time of the design of the processing system and at the time of the processing itself to maintain security and prevent unauthorised processing, taking into account the risks represented by the processing and the nature of the data.

The personal information a user posts online, combined with data outlining the users' actions and interactions with other people, can create a rich profile of a person's interests and activities. Personal data published on social network sites can be used by third parties for a wide variety of purposes, including commercial purposes, and may pose major risks such as identity theft, financial loss, loss of business or employment opportunities and physical harm.

Of paramount importance, SNS providers should inform users of their identity from the outset and outline all the different purposes for which they process personal data in accordance with section 22 of the Data Protection Act. Particular care should be taken by SNS providers with regard to the processing of the personal data of minors.

SNS providers and third party application providers are most of the time data controllers with corresponding responsibilities towards users. Section 54 of the Data Protection Act on 'Domestic purposes" will apply to SNS such that personal data processed by an individual for his personal, family or household affairs or for recreational purposes would be exempt from certain provisions of the Act. The dissemination and use of information available on SNS for other secondary, unintended purposes is of key concern to the office. Robust security and privacy-friendly default settings are advocated throughout the guide as the ideal starting point with regard to all services on offer.

Applicability of DPA

SNS providers are considered data controllers under the Data Protection Act even if their headquarters are based for example outside Mauritius. They provide the means for the processing of user data and provide all the "basic" services related to user management (e.g. registration and deletion of accounts). SNS providers also determine the use that may be made of user data for advertising and marketing purposes – including advertising provided by third parties.

Obligations of SNS

- **SNS should inform users of their identity, and provide comprehensive and clear information about the purposes and different ways in which they intend to process personal data.**
- **SNS should offer privacy-friendly default settings.**
- **SNS should provide information and adequate warning to users about privacy risks when they upload data onto the SNS.**
- **Users should be advised by SNS that pictures or information about other individuals should only be uploaded with the individual's consent.**
- **At a minimum, the homepage of SNS should contain a link to a complaint facility, covering data protection issues, for both members and non-members.**
- **Marketing activity must comply with the rules laid down in the Data Protection Act.**
- **SNS must set maximum periods to retain data on inactive users. Abandoned accounts must be deleted.**
- **Users should, in general, be allowed to adopt a pseudonym.**
- **With regard to minors, SNS should take appropriate action to minimise risks.**

A large proportion of SNS services are utilised by children/minors. There is thus a need for taking into account the best interest of the child as also set out in the UN Convention on the Rights of the Child. Based

on the considerations made so far, a multi-pronged strategy would be appropriate to address the protection of children's data in the SNS context.

Such a strategy might be based on:

- awareness raising initiatives, which are fundamental to ensure the active involvement of children (via schools, the inclusion of DP-basics in educational curricula, the creation of ad-hoc educational tools, the collaboration of national competent bodies);
- fair and lawful processing with regard to minors such as not asking for sensitive data in the subscription forms, no direct marketing aimed specifically at minors, the prior consent of parents before subscribing, and suitable degrees of logical separation between the communities of children and adults;
- implementation of Privacy Enhancing Technologies (PETs) - e.g. privacy-friendly settings by default, pop-up warning boxes at appropriate steps, age verification software;
- self-regulation by providers, to encourage the adoption of codes of practice, under the guidance of the Data Protection Commissioner, that should be equipped with effective enforcement measures, also disciplinary in nature.

Rights of Users

Both members and non-members of SNS have the rights of data subjects, wherever applicable, according to the provisions of the Data Protection Act.

Many SNS allow users to contribute data about other people, such as adding a name to a picture, rating a person, listing the "people I have met/want to meet" at events. This tagging may also identify non-members. However, the processing of such data about non-members by the SNS may only be performed if the criteria laid down in the Data Protection Act are fulfilled. In addition, the creation of pre-built profiles of non-members through the aggregation of data that is independently contributed by SNS users, including relationship data inferred from uploaded address books, lacks a legal basis.

Both members and non-members should have access to an easy-to-use complaint handling procedure set up by the SNS. Members and non-members of SNS must have a means to exercise their right of access, correction and deletion.

Third party access

SNS-mediated access

In addition to the core SNS service, most SNS offer users additional applications provided by third party developers who also process personal data as data controllers or processors.

SNS should have the means to ensure that third party applications comply with the Data Protection Act. This implies, in particular, that they provide clear and specific information to users about the processing of their personal data and that they only have access to necessary personal data. Therefore, layered access should be offered to third party developers by the SNS so they can opt for a mode of access that is intrinsically more limited. SNS should ensure furthermore that users may easily report concerns about applications.

User-mediated third party access

SNS sometimes allow users to access and update their data with other applications. For example, users might be able to:

- read and post messages to the network from their mobile phones;
- synchronize the contact data of their friends in the SNS with their address books on a desktop computer;
- update their status or location in the SNS automatically by using another website.

This software can be written in the form of an "Application Programming Interface" ("API") which refers to access whereby users need to provide their login credentials to the software, so that it can act on their behalf.

This enables any third party to write software to perform these tasks, and allow users to freely choose between several third party providers. When offering an API that enables access to contacts' data, SNS should provide for a level of precision that lets the user choose an access level for the third party that is just sufficient to perform a certain task.

When accessing personal data via third party's API on behalf of a user, third party services should:

- **process and store data no longer than necessary to perform a specific task;**
- **perform no operations on imported user contacts' data other than personal usage by the contributing user.**

Some SNS allow their users to send invitations to third parties. The practice by some SNS to send invitations indiscriminately to the entire address book of a user is not allowed. Some SNS also retain identification data of users who were banned from the service, to ensure that they cannot register again. In that case, these users must be informed that such processing is taking place. In addition, the only information that may be retained is identification information, and not the reasons why these persons were banned.

Personal data communicated by a user when he registers to a SNS should be deleted as soon as either the user or the SNS provider decides to delete the account. Similarly, information deleted by a user when

updating his account should not be retained. SNS should notify users before taking these steps with the means they have at their disposal to inform users about these retention periods. For security and legal reasons, in specific cases, it could be justifiable to store updated or deleted data and accounts for a defined period of time in order to help prevent malicious operations resulting from identity theft and other offences or crimes.

When a user does not use the service for a defined period of time, the profile should be set to inactive, i.e. no longer visible to other users or the outside world, and after another period of time the data in the abandoned account should be deleted. SNS should notify users before taking these steps with whatever means they have at their disposal.

SEARCH ENGINES

Fig 5: Search engines

Search engine providers undeniably fulfill a pivotal role in the digital age as intermediaries on the World Wide Web. However, data protection concerns should also be addressed when delivering internet-based services. The primary objective throughout this guide is to strike a balance between the legitimate business needs of search engine providers and the protection of the personal data of internet users.

First, in their role as service providers to the users, search engines collect and process vast amounts of user data, including data gathered by technical means, such as cookies. Data collected can range from the IP address of individual users to extensive histories of past searching behaviour or data provided by users themselves when signing up to use personalised services. Search engines in their role as collectors of user data must sufficiently explain the nature and purpose of their operations to the users of their services.

Second, in their role as content providers, search engines help to make publications on the internet easily accessible to a worldwide audience. Some search engines republish data in a so-called 'cache'. By retrieving and grouping widespread information of various types about a single person, search engines can create a new picture, with a much higher risk to the data subject than if each item of data posted on the internet remained separate. The representation and aggregation capabilities of search engines can significantly affect individuals, both in their personal lives and within society, especially if the personal data in the search results are incorrect, incomplete or excessive.

The danger lies in the invention or re-moulding of an image of an individual which may be totally misconceived or which the individual himself would not like to share in his legitimate right with the world. It is not an excuse for the data controller to invoke the voluntary provision of personal information by individuals who are not aware of the use/s made of or to this information. The legal requirement of "express consent" cannot be met in this way.

The express consent of the user must be sought for all use/s of his/her data including profile enrichment exercises. Opt-outs facilities must be provided by search engines and requests from users to update/refresh caches must be complied with.

Applicability of DPA

- The Data Protection Act generally applies to the processing of personal data which is carried out in Mauritius by search engines, even when their headquarters are outside Mauritius. Article 3 of the Act clearly states that the DPA is applicable when a data controller who is not established in Mauritius but uses equipment in Mauritius for processing data, other than for the purpose of transit through Mauritius. Any person who is ordinarily resident in Mauritius and carries out data processing activities through an office, branch or agency in Mauritius, is treated as being established in Mauritius.

- Search engine providers should inform their users about compliance with the Data Protection Act, whether by establishment or by use of equipment.

Obligations on search engine providers

- **Search engines may only process personal data for lawful and necessary purposes and the amount of data has to be relevant and not excessive in respect to the various purposes to be achieved.**

- **Search engine providers must delete or anonymise personal data in an irreversible manner once they are no longer necessary for the purpose for which they were collected. The development of appropriate anonymisation schemes by search engine providers is recommended. Anonymisation of data should exclude any possibility of individuals to be identified, even by combining anonymised information held by the search engine company with information held by another stakeholder (for instance, an internet service provider).**

- **Retention periods should be minimised and be proportionate to each purpose put forward by search engine providers. Search engine providers should implement the principle of "privacy by design", i.e, through the adoption of privacy-enhancing technologies, which will additionally contribute to further reduce the retention period. In addition, a reduced retention period will increase users' trust in the service and will thus constitute a significant competitive advantage.**

- **While search engine providers inevitably collect some personal data about the users of their services, such as their IP address, resulting from standard HTTP traffic, it is not necessary to collect additional personal data from individual users in order to be able to perform the service of delivering search results and advertisements.**

- **If search engine providers use cookies, their lifetime should be no longer than necessary. Similarly to web cookies, flash cookies should only be installed if transparent information is provided about the purpose for which they are installed and how to access, edit and delete this information.**

- **Search engine providers must give users clear and intelligible information about their identity and location and the data they intend to collect, store or transmit, as well as the purpose for which they are collected.**

- **Enrichment of user profiles with data not provided by the users themselves is to be based on the express consent of the users.**

- **Search engines should respect website editor opt-outs indicating that the website should not be crawled and indexed or included in the search engines' caches.**

- **When search engine providers provide a cache, in which personal data are being made available for longer than the original publication, they must respect the right of data subjects to have excessive and inaccurate data removed from their cache.**

- **Search engine providers that specialise in the creation of value added operations, such as profiles of natural persons (so called 'people search engines') and facial recognition software on images must have a lawful ground for processing, such as express consent, and meet all other requirements of the Data Protection Act, such as the obligation to guarantee the quality of data and fairness of processing.**

Rights of users

- Users of search engine services have the right to access, inspect and correct if necessary, all their personal data, including their profiles and search history.

- Cross-correlation of data originating from different services belonging to the search engine provider may only be performed if express consent has been granted by the user for that specific service.

GLOSSARY

Alphanumeric

Alphanumeric is a combination of alphabetic and numeric characters, and is used to describe the collection of Latin letters and Arabic digits or a text constructed from this collection. There are either 36 (single case) or 62 (case-sensitive) alphanumeric characters. The alphanumeric character set consists of the numbers 0 to 9 and letters A to Z.

Click-through

Click-through rate or CTR is a way of measuring the success of an online advertising campaign. The CTR for an ad is defined as the number of clicks on an ad divided by the number of times the ad is shown (impressions), expressed as a percentage. For example, if a banner ad was delivered 100 times (100 impressions) and received one click then the CTR would be 1%.

Click trails

Click trails consist of information about an individual's behaviour, identity, pathway or choices expressed while visiting a web site. They contain the links that a user has followed and are logged in the web server.

Cookie

A cookie (HTTP cookie or browser cookie) is a small file of letters and numbers downloaded on to your computer when you access certain websites. It allows a website to recognise a user's computer. Cookies themselves do not require personal information to be useful and, in most cases, do not personally identify internet users. Cookies are used in behavioural advertising to identify users who share a particular interest so that they can be served more relevant adverts.

Data Controller

A person who, either alone or jointly with any other person, makes a decision with regard to the purposes for which and in the manner in which any personal data are, or are to be, processed.

Data Processor

A person, other than an employee of the data controller, who processes the data on behalf of the data controller.

Hyperlinks

A hyperlink (or link) is a reference to a document that the reader can directly follow, and points to a whole document or to a specific element within a document. Hypertext is text with hyperlinks. A user following hyperlinks is said to navigate or browse the hypertext. For example, in an online reference work such as Wikipedia, many words and terms in the text are hyperlinked to definitions of those terms.

Network Provider

An Internet service provider (ISP) is a company that provides access to the Internet. Access ISPs directly connect customers to the Internet using copper wires, wireless or fiber-optic connections.

Online Behavioural Advertising

A technique used to make use of information about web-browsing behaviour to deliver advertisements tailored to individuals' interests. It is also known as behavioural targeting, interest-based advertising or ad-matching.

Operating System

An operating system (OS) is a set of programs that manages computer hardware resources, and provides common services for application software. The operating system is the most important type of system software in a computer system. Without an operating system, a user cannot run an application program on his computer, unless the application program is self booted.

Opt-in

Opt in e-mail is a term used when someone is given the option to receive "bulk" e-mail, that is, e-mail that is sent to many people at the same time. Typically, this is some sort of mailing list, newsletter, or advertising. Obtaining permission before sending e-mail is critical because without it, the e-mail is known as spam.

Opt-out

The term opt-out refers to several methods by which individuals can avoid receiving unsolicited product or service information. This ability is usually associated with direct marketing campaigns such as telemarketing, e-mail marketing, or direct mail.

Publishers

Publishers rent out space on their websites for ad networks to place adverts.

Search Engines

A web search engine is designed to search for information on the World Wide Web and present the results. The information may consist of web pages, images, information and other types of files. Search engines operate algorithmically or are a mixture of algorithmic and human input.

Social Networking Sites

A social networking site is online and focuses on building and reflecting of social networks among people, who, e.g., share interests and/or activities. They are web based and provide means for users to interact over the Internet, such as e-mail and instant messaging. Social networking sites allow users to share ideas, activities, events, and interests within their individual networks.

Tailored Advertising

Targeted advertising is a type of advertising whereby advertisements are placed so as to reach consumers based on various traits such as demographics, purchase history, or observed behaviour.

User-mediated

Action that is triggered by the user himself.

Web Browsers

A web browser can be defined as an application software or program designed to enable users to access, retrieve and view documents and other resources on the Internet. Although browsers are primarily intended to access the World Wide Web, they can also be used to access information provided by web servers in private networks or files in file systems.The major web browsers are Internet Explorer, Firefox, Google Chrome, Safari, and Opera.

Web Page

A web page or webpage is a document or information resource that is suitable for the World Wide Web and can be accessed through a web browser and displayed on a monitor or mobile device. This information is usually in HTML or XHTML format, and may provide navigation to other web pages via hypertext links.

Web Server

Web server can refer to either the hardware (the computer) or the software (the computer application) that helps to deliver content that can be accessed through the Internet. The most common use of web servers is to host web sites but there are other uses like data storage or for running enterprise applications.

World Wide Web

The World Wide Web (WWW or the Web) is a system of interlinked hypertext documents accessed via the Internet. With a web browser, one can view web pages that may contain text, images, videos, and other multimedia and navigate between them via hyperlinks.

REFERENCE

http://windows.microsoft.com/en-US/internet-explorer/products/ie/home

http://www.mozilla.org/en-US/firefox/new

http://www.google.com/chrome

http://www.apple.com/safari

http://office.microsoft.com

http://www.youronlinechoices.com/what-is-behavioural-advertising

http://www.cdt.org/content/behavioral-advertising-across-multiple-sites

http://www.searchengineready.co.uk

http:// www.searchengineoptimizationcompany.ca

http://www.youronlinechoices.com/uk/jargon-buster

http://en.wikipedia.org/wiki/Behavioral_advertising

http://www.parikiaki.com/archives/25396

http://singularityhub.com/category/artificial-intelligence/?count=40

Contact Details:

Tel: 201 3604
Email: pmo-dpo@mail.gov.mu
Website: http://dataprotection.gov.mu

Designed and Printed: Government Printing Department, June 2012