

Client in the web (summary)

Introduction

Internet offers amazing possibilities to obtain information on goods and services. It involves several parties; telecom companies provide the essential connections, Internet service providers provide Internet access and suppliers such as Internet site managers provide various services. Sometimes an organisation might fulfil different functions.

Internet offers many possibilities. Users might for instance surf the world wide web (WWW), send and receive e-mails, chat with each other, join news or discussion groups, telephone online, and so on. It is also possible to develop and maintain Internet sites.

Instead of direct routes, messages sometimes make detours to reach a particular destination. Once users start 'surfing', the necessary data travel through a number of channels (portals, routers, etc.) to the manager of the site in question. Technically, all of these Internet junctions can retain passing information for private use.

Besides this, some of these parties possess certain details arising from a relationship with the user. Internet providers usually possess the names and addresses of parties who access Internet through them. Internet site managers who also offer products or services will also possess specific details of clients who have accepted their offers. Providers offering e-mail facilities save messages in the user's 'electronic mailbox'. The user can only access his electronic mail after he logs in.

This research focuses on the relationship between the consumer and the provider offering Internet access. We first describe the nature of this relationship and some relevant details, after which a legal framework is presented for lawful use of those details.

Research setup

At the end of December 1999 the Dutch Data Protection Authority (Registratiekamer) wrote to 60 providers about its intention to study how Internet providers collect and use personal details. In doing so the Registratiekamer used the NLIP list of members (available on the NLIP Internet site), its own registration file, messages from the media along with its own Internet expertise.

In its letter the Registratiekamer requested providers to fill in the enclosed questionnaire and send it back within three weeks. The letter has been included in this report in appendix 1. By the end of this period only some providers had reacted. By the end of January 2000 the Registratiekamer sent letters of recall offering providers a two-week term. About one-quarter of the providers had not received the letter of 23 December 1999. Some providers claimed they had lost the letter. As a result of this most reactions were not received until the end of February 2000. Consequently the research was behind planning. A small number of providers did not react despite repeated telephone requests.

At first, the Registratiekamer based its findings on respondents' answers to the questionnaire. Information material such as general conditions, information brochures and privacy statements which the providers had sent to the Registratiekamer was also used. Supplementary to the questionnaire, the Registratiekamer carried out fact-finding studies on a number of representative suppliers of Internet services. Comparing the answers and the information material to the Telecom Act, the Personal Registration Act and the Data Protection Act, a general idea developed on how providers treat personal details. This idea was processed in frames in the report. Rules developed on the basis of frames and findings. In the last phase of the research, each respondent was informed separately on the findings relevant for his company.

Findings

The role of the provider

Most access providers have their own home pages which also function as portals for Internet surfing. Most providers do not distinguish the various functions.

Knowing the client

The content provider can calculate exactly how many advertisements (banners) of a certain type have been placed, how often the user has visited the e-shop and which articles have been sold for how much money. Content providers use cookies on a regular basis. This usage falls outside the scope of this study.

(General) conditions

Almost all providers maintain general conditions. Those who do not still set conditions to using the service offered. They have been indicated in general terms on the registration form to be filled in by the applicant. So there are always some restrictions regarding the use of the services offered. The conditions set by providers in the general conditions might regard paying method, the use of the service offered and, for instance, the way in which the subscriber's personal details are used. In case of providers offering free Internet access (the so-called free providers), we are dealing with the 'one good turn deserves another' principle. Although the subscriber does not pay to use the services offered, he does however submit to a specified use of his personal details. Free and 'non-free' Internet providers (to be referred to as paid providers) often include conditions related to the use of personal details in their general conditions. None of the questioned providers has mentioned the agreement consequences if the user objects to the use of some of his personal details. Apparently this is not essential to the agreement.

Differentiating free and non-free

The information material sent by providers shows that there is not always a distinction between free and paid providers. Some paid providers offer free Internet access whereas some free providers also have non-free subscriptions. Some of the providers maintain the same general conditions for different subscription forms, which makes it difficult to make this distinction.

Basic details

Most providers ask for the subscriber's basic details (name, address and place of residence). Internet access is not offered without these details. Paid providers also need the subscriber's account number. Free providers in particular ask for the applicant's operating system, his hobbies and interests. Paid providers are also interested in the applicant's training and operating system. If the provider is also offering e-mail facilities while the subscriber has an e-mail address, this too is considered a personal detail. It is easier to identify the subscriber using his basic details.

The striking thing is that some of the free providers collect the basic details by simply posting the information necessary to call in to the potential subscriber. Many of these free providers save the details after they have been sent, unnecessarily. The question is to what extent do these free providers consider the saving of these details to be essential to the relationship with the subscriber. In such cases it is not always emphasised that details are saved after they have been sent (and for what purposes).

Traffic details

Many providers have indicated that they save traffic details (details on the actual use of the Internet services offered) in all functions. The remarkable thing here is the confusion about this concept. Paid and free providers save the log-in information and times, the IP address and the nature of the service obtained (protocol used). There is a great difference in the saving period of these details, varying from a few days to an indefinite period. Most of these details are not analysed individually, according to providers' answers and information material. One of the

reasons given is that it takes too much capacity. Providers, however, do use 'anonymous' or aggregated information to improve performance. To settle the message traffic, access providers do not need to know the contents. Some of the respondents felt free to indicate that they did not save the communication contents.

Providers carry out different policies when saving traffic details. The reason to save these details is often unknown. Some paid providers use these details for marketing purposes. The same goes for a number of free providers. Now, what is meant by 'marketing purposes'? Details and available information often do not provide clear answers, they are even contradictory.

Many providers studied by the Registratiekamer save some of the traffic details. Subscribers' account details make it easy to identify the subscribers. The fact that this happens has also been indicated by the providers themselves, for instance when asked by the police/justice to cooperate in a criminal case research (racism, child pornography, etc.) committed by a subscriber on the Net.

Objectives

Providers have listed many possible objectives. For instance dealing with complaints, detecting fraud, traffic control, collection purposes and security. Some of the objectives were general and/or comprehensive to such extent that we could not possibly draw any conclusions. Examples are "carrying out a sound management" and "administrative processing". Each provider formulates these objectives differently, often indistinctly. The information on the intended objective given to the (potential) subscriber is obscure and often unequivocal.

In their general conditions some of the providers mention objectives different from the ones in the set-up privacy statement. The aim of the registration form often deviates from the other information offered to the subscriber. Some providers have told the Registratiekamer different objectives than the ones formulated in the submitted documents.

Many providers collect personal details to somehow approach their subscribers in a personal way. Sometimes this happens without informing the subscriber. If the subscriber has been informed, the objective is formulated in a quite different, often obscure way. It is often not clear whether it is only the provider who approaches the subscriber, or whether others are also contacting the subscriber via the provider; if so, who are the 'others'.

Forwarding information to third parties

The striking thing is that quite many providers do not consider forwarding subscriber's details within group context, to shareholders or related companies with whom a joint venture has been entered into, to be forwarding details to third parties. This is a misconception according to fixed statements by the Registratiekamer. It is therefore only natural that information in this regard sent to (potential) subscribers is unclear, if not incorrect. Again, information offered by providers on this matter is not unequivocal.

Conditions

Free and paid providers do not always indicate clearly the details to be submitted by the subscriber and the details he may reveal. Paid providers declared regularly that this distinction does not have to be made as these details are not essential. Providers do make this distinction in case of online registration, but not in case of offline registration. As the function of the access provider is not always easy to distinguish from the function of the content provider, it remains unclear which details are collected for what purposes.

One of the conditions set by many providers, is the use of subscriber details to be able to approach the subscriber with (commercial) offers (direct marketing purposes). Subscriber details used to this end are usually the details the subscriber fills in upon registration. This does not

concern basic details only, but also other information such as education, family situation, personal preferences etc. The agreement develops even if the subscriber does not enter these details. Therefore such conditions cannot be regarded as main stipulations. The basis to process these details is not the necessity to execute the agreement.

Some of the providers request the subscriber to allow for his personal details to be used for direct marketing purposes. Such description is far from specific and clear-cut to talk of subscriber permission.

Some of the providers point the potential subscriber explicitly to the general conditions which apply during the software installation. The subscriber can only install the software having clicked the right button to confirm his familiarity with the presented general conditions and to agree to the included stipulations. Insofar the conditions comply with the intrinsic requirements of unambiguous permission, one can defend the fact that in doing so the subscriber indeed grants permission for details processing.

Privacy statement or protocol

In general, providers use the general conditions to point (potential) subscribers out to the further use of their details. It is more often free providers who use a privacy statement/protocol. In most cases information is supplied both ahead of and subsequent to the registration. Providers hardly ever make a distinction between the processing of account and traffic details. Besides, the objectives formulated by providers for the processing of details are not unequivocal and often unspecified.

Client's rights

A small number of providers attract the subscriber's attention to his right to view and correct his details. Some of the providers offer their subscribers the possibility to use their right to view, correct and delete details online. Many providers do not emphasise the subscribers' right to object to their details being used for unspecified direct marketing purpose until they have registered and online.

Security

Most providers are not responsible for securing personal details.

Presenting file to the Registratiekamer

More free (small majority) providers have presented their files to the Registratiekamer than paid providers (minority). Despite requests to do so, providers who have not presented their files, have not indicated in general which exemption facility they appeal to. Providers who have presented their personal registrations to the Registratiekamer mainly use the general conditions to inform their subscribers.

Conclusion

It can be concluded from the findings that there is much obscurity about saving and using personal details by providers and that providers often do not realise the rules protecting their subscribers' privacy. The reason for personal details to be collected and used is often unknown or ambiguous. This also goes for announcements made to (potential) subscribers in this regard. Furthermore, it is not always clear in what function providers carry out their activities, and what the relationship is between the intended objectives and the details saved to this end. It remains to be seen whether the saved details are really necessary to realise these objectives.

In some cases providers use traffic details to approach their subscribers. Some of the providers have indicated their intention to do so. Insofar the provider uses traffic details which he has saved as being the access provider, this is only permitted to a limited extent. In these cases the

Registratiekamer establishes that the subscriber has not granted the legally required permission to keep such details once the Internet session has terminated. Due to the unclear functions in which providers carry out their activities, the Registratiekamer has great doubts about the rightfulness of saving (and using) these details for marketing purposes.

Providers only mention in dribs and drabs the subscribers' rights on the basis of the privacy legislation and how to use these rights.

With regard to the observance of the requirements set by the Personal Registration Act for a sound use of subscribers details, in general the Registratiekamer did not observe any major differences between free and paid providers.

It follows on the preceding that, when offering Internet access, providers maintain unclear and contradictory or even unlawful objectives for the use of subscribers' personal details. This makes it difficult for the subscriber to obtain insight into how the provider treats his details. The title of this study, *Client in the Web*, therefore illustrates the consumer's very limited possibilities to interfere with the use of his details.

In general and based on its research, the Registratiekamer draws the conclusion that providers fail considerably in the protection of personal details when using Internet. To improve this providers should take the following rules into consideration.

Internet access rules

In the previous chapters we have given a description of providers' activities when offering Internet access; we have also outlined the legal frame for the protection of the user's privacy for the Internet services offered by the provider. Combining the activities and the legal frame, rules can be formulated for an efficient privacy policy when offering Internet access. These rules are as follows:

1. Providers must realise the functions in which they carry out certain activities and save details for what purposes. Here we distinguish the following functions:
 - A. Provider as Telecom company.
 - B. Access provider.
 - C. Content provider.
 - D. Web hosting provider.
2. Providers offer Internet access as access providers. To this end and to run the system it is necessary to save login name, user password and the assigned IP address. These details can be deleted once the Internet session has terminated. Providers also need to save users' e-mail addresses if using e-mail facilities.
3. Details registered and saved by providers are determined by the technical necessity and the conditions set by the providers themselves to the subscribers to use the services offered. Here the subscription type is also pivotal for offering Internet access. We distinguish three varieties:
 - A. Internet access at subscription fee.
 - B. Free access with registration fee.
 - C. Free access.
4. Providers should realise when to collect details, what kind of details to collect and how long to keep them. We distinguish:
 - A. The contents of messages; providers may not take note of the contents of messages, unless they are sent to them.

- B. Details regarding the use of Internet services (traffic details) that cannot lead to the identification of a natural person (personal details).
- C. Traffic details that are also personal details.
- D. Personal details that are not traffic details.

5. Access providers may not save and use traffic details, unless one of the conditions of article 11.5, paragraph two, of the Telecom Act has been complied with. If these exceptions are not applicable, access providers are to destroy or 'anonymise' the traffic details once the Internet session has terminated. This applies even if the subscriber has given permission for a different use of these details.

One of the exceptions determines that access providers have the right to save traffic details for their own marketing activities provided the following conditions have been complied with:

- A. Processing is necessary to carry out the marketing activity.
- B. It regards a marketing activity of the provider himself.
- C. The subscriber has given permission to do so.

6. Pursuant to article 11.5 of the Telecom Act, traffic details that are also personal details and which are kept by access providers, may only be processed insofar the stipulations of the privacy legislation are observed.

7. The various objects intended by collecting subscribers' personal details must be distinguished and specified. Communication in this regard must be unequivocal.

8. Once subscriber details have been collected for marketing purposes, it must be indicated what these activities comprise. The following division is usually maintained:

- A. Providers approaching subscribers with information on their own products and services.
- B. Providers approaching subscribers with information on products and services of third parties.
- C. Supplying details to enable others to approach subscribers. Should the occasion arise, it must be noted that the registered details are analysed to link the message sent to the subscriber's preferences and/or interests.

9. There should be a clear relationship between the objectives and the personal details necessary to realise this. Providers must distinguish:

- A. Details to be submitted by subscribers to use the Internet services offered.
- B. Details requested by the provider and used for purposes other than offering primary Internet services. It must be indicated to what extent subscribers are compelled to submit this information, for instance on the registration form.

10. Providers must determine the basis for processing details. This might be:

- A. The necessity to be able to carry out the agreement. In that case the determining condition must be qualified as a main stipulation that is essential to the agreement between the provider and the subscriber.
- B. The subscriber's clear-cut permission that should comply with the following conditions:
 - i. The subscriber should be able to express his will in all freedom; this will must be actually expressed.
 - ii. The expression of will must be related to a certain details processing or to a limited category of details processing.
 - iii. The subscriber must have the necessary information at his disposal to be able to grant permission (informed consent). The subscriber can always withdraw his permission.
- C. The provider's justified interest. Insofar the stipulations in the Telecom Act allows for this, providers generally have a justified interest in approaching their subscribers with commercial or charitable messages. Insofar he has not agreed about this yet with the subscriber or insofar he does not have the subscriber's permission yet, his privacy should be taken into consideration. Explicit announcements in this regard to the (potential) subscriber are significant indications.

11. One condition stating that the subscriber agrees to his personal details being used for direct marketing purposes in general does not comply with the requirements for granting permission as referred to in the Data Protection Act. This can only be different provided this condition is a main stipulation recognised and accepted by the subscriber as such. Adding a special square enabling the subscriber to agree to a specified processing of his details, does comply with the conditions for granting permission.

12. If, with the lapse of time, providers want to use the personal details to realise objectives other than the ones specified when collecting those details, they must judge whether the new intended processing is consistent/inconsistent with the original objectives. Five criteria must be considered in mutual connection:

- A. The relationship between the aim of the details processing and the reason to obtain details.
- B. The nature of the sensitivity of the relevant details.
- C. Whether decisions can be taken that will effect the subscriber.
- D. How details are obtained.
- E. The extent to which the party involved receives appropriate securities.

13. Before registering the potential subscriber, he should be informed by the provider on his identity and the purposes of processing personal details. To make sure personal details are processed decently and accurately more information is sometimes needed like the party receiving the details and how the subscriber can exercise his rights. This is possible via general conditions sent to subscriber (for instance attached to the CD-ROM installation), or which he can read online before he registers.

A separate Internet page with a privacy statement on which the provider submits his privacy policy and which can be accessed through a button on the provider's homepage, offers this possibility to increase the transparency regarding the use of personal details at limited expenses.

14. Providers must respect the right to view, track, correct and delete subscriber details and enable him to use this right.

15. Subscribers have the right to lodge an objection against specified processing of his personal details. In such case providers are bound to abandon the intended processing if it regards a direct marketing purpose.

Subscribers should have the possibility to object to details processing intended for direct marketing purposes easily and at low expenses. For instance by enabling the subscriber to tick off when applying for a subscription.

Providers should emphasise the possibility to object to incoming mailings/messages upon sending commercial or charitable messages. This obligation does not apply when sending newsletters with remarks regarding the primary sector as well as commercial messages.

16. Providers are to make sure the details processes are efficient and relevant for the objectives. The details also need to remain complete, accurate and up-to-date. In addition, personal details must be destroyed if no longer necessary for the objectives. Providers should therefore wonder (regularly) whether there is any reason why they should keep details. Providers may only keep personal details within a set restrictive term.

17. Providers must take technical and organisational measures to protect personal details against loss or any form of unlawful processing. This also means that the party responsible must arrange his systems as such to reduce the chance of personal details being collected and processed unlawfully. Applying Privacy Enhancing Technologies is an option.

18. Providers are compelled to report the process to the Personal Data Protection Board (Dutch DPA). It is possible, however, to release some of the processings from this obligation. They have been referred to in the exemption decree. Having introduced the Data Protection Act a floppy disk is available at the Dutch DPA, which enables the user to judge whether exemption is applicable for to this details processing. If not, the floppy disk can be used to fill in the registration form. The printout can be sent to the Dutch DPA.