

# Privacy Enhancements in the Mobile Internet

Mikael Nilsson\*, Helena Lindskog\*, Simone Fischer-Hübner

Karlstad University  
Department of Computer Science  
SE-651 88 Karlstad  
Sweden  
{micke, helena, simone}@cs.kau.se

**Abstract.** While the mobile Internet makes available location-based as well as other useful services to the mobile users, risks to the user's privacy have to be taken into consideration as well. Personal user data, such as traffic data, location data, device and user specific capability and preference information, and content data is exposed at different sites, such as the WAP Gateway/Proxy or the Origin Server's sites. In this paper, we first define privacy and basic privacy requirements and analyze privacy risks in the mobile Internet environment. We especially investigate those generated by the use of device and user specific profiles. Furthermore, we discuss technical means for enhancing privacy. Particularly, we show how the Platform for Privacy Preferences Project (P3P) protocol can be used to enforce the user's control over the release of location data and capability and preference information, and how it can be enhanced.

**Keywords:** *mobile Internet, privacy, profiles, CC/PP, P3P, WAP, privacy enhancing technologies*

## 1 Introduction

In a very short time, the mobile Internet has grown into immense proportions. Its mechanisms allow users both to access the Internet services and other server-based applications from mobile devices, and make new services possible, such as location-based and context-aware applications. Today, WAP (Wireless Application Protocol) and iMode are the most frequently used technologies besides standard HTML over modified TCP/IP used in most Personal Digital Assistants (PDA). While mobile web services can be of great use, the privacy risks have to be considered, and appropriate data protection and privacy safeguards must be ensured. It is necessary to prevent

---

\* The authors are also with Ericsson Infotech, Box 1038, SE-651 15 Karlstad, Sweden.

mobile Internet users to be under permanent surveillance and that the only possibility for them to protect their privacy is not to use the mobile services at all.

The Composite Capability/Preference Profiles (CC/PP) specification is a working draft by the World Wide Web Consortium (W3C), which forms a framework for definition of capabilities and preferences associated with users and user agents in Internet networks. CC/PP is intended to help structure information necessary to adapt the content and the content delivery mechanisms to best fit the capabilities and preferences of the users and user agents. The User Agent Profile (UAProf) specification by the WAP Forum [WAP], which extends the CC/PP standard, also defines the user location as a reserved attribute. However, the planned transmission of device and user specific Capability and Preference information (CPI) also raises privacy and security questions that have to be adequately addressed.

Specific legal provisions to protect privacy in the mobile web are needed in addition to existent general data protection legislation. However, privacy is increasingly becoming an international problem, since communication data often crosses state borders. An international harmonization of privacy legislation is necessary, but hardly achievable due to cultural differences (see also [Fischer-Hübner 2000]). The recent transatlantic debate about the adequacy of the Safe Harbor privacy principles in comparison with the EU Data Protection Directive has demonstrated the difficulty of harmonizing data protection regulations. For this reason, and also because law is not an ultimate protection, it is important to enforce privacy also by technology. Hence, privacy-enhancing technologies for protecting the mobile web users have to be developed.

At Karlstad University, we investigate privacy and privacy risks in the mobile Internet, as well as technical means for enhancing the user's privacy. This paper presents the first project results.

After defining privacy and basic privacy requirements, privacy risks, especially those generated by the use of location data and user device specific profiles, are analyzed, and exemplified with misuse scenarios. We also propose how to use the Platform for Privacy Preferences (P3P) protocol by the W3C to protect CPI and location data and discuss how P3P can be combined and enhanced with other security mechanisms. We have investigated the problems and solutions in WAP systems, but the same ideas will hold for other mobile Internet architectures, such as iMode.

## **2 Privacy**

Privacy is well recognized as a fundamental human right. The most common definition of privacy in current use is the one by Alan Westin: "Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others" [Westin 1967].

The emphasis of this paper is on the discussion of informational privacy of individuals. In order to protect this right of informational self-determination, data protection laws of mostly western states as well as international privacy guidelines or directives (such as the EU-Directive 95/46/EC on Data Protection [EU Directive 1995]) and the OECD Privacy guidelines [OECD 1980], require basic privacy

principles to be guaranteed when personal data are collected or processed. These include:

- *Legitimacy*: Personal data collection and processing is only admissible if permitted by legal provisions or if the data subject has consented (Art. 7 EU Directive);
- *Purpose specification and purpose binding*: personal data must be obtained for specified and legitimate purposes and should not be used for other purposes (see Art. 6 EU Directive);
- *Necessity of data collection and processing*: the collection and processing of personal data shall only be allowed, if it is necessary for the tasks falling within the responsibility of the data processing agency (see Art. 7 EU Directive);
- *The data subject's right to information, notification, objection and the right to correction, erasure or blocking of incorrect or illegally stored data* (see Art. 10 - 14 EU Directive);
- *Supervision and sanctions*: control for compliance by an independent supervisory authority (see Art. 28 EU-Directive). Criminal or other penalties should be envisaged in the event of non-compliance; and
- *Requirement of adequate technical and organizational security mechanisms* to guarantee the confidentiality, integrity, and availability of personal data (see Art. 6, 17 EU-Directive).

The privacy enhancing security criteria of anonymity or pseudonymity of a user is derived from the necessity principle. The privacy principle of necessity of data collecting and processing means that personal data should not be collected or used for identification purposes when not really necessary. Consequently, information systems should guarantee that, if possible, users can act anonymously. The best design strategy to enforce this requirement is the avoidance or at least minimization of personal data.

Provisions of the EU-Directive 95/46/EC on Data Protection as well as national data protection laws also apply to the collection and processing of personal data in the mobile Internet environment. Nevertheless, more specific privacy requirements for the mobile Internet environment were recently formulated in the Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communication sector [EU Directive-Proposal 2000]. This proposed new directive is intended to replace the directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunication sector [EU-Telecommunication Directive 1997] and in contrast to directive 97/66/EC has an extended scope to apply to both the classic telecommunication sector as well as the Internet sector. In addition to the protection of traffic data, the directive addresses also location data giving the geographic location of mobile users or, more precisely, of their devices. According to Art.9 I, location data may only be processed when it is anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. Also, according to Art.9 II, where consent of users has been obtained, the user must continue to have the possibility of temporarily refusing the processing of location data for each connection to the network, or for each transmission of the communication. Exceptions are formulated for emergency services.

### **3 Mobile Internet Architecture, Technologies and Services**

This chapter describes the fundamentals of mobile Internet environments and services.

#### **3.1 Mobile Network Architecture**

A second-generation mobile network comprises a set of components, organized in a network that can perform the necessary switching, and contains all the information necessary about users and links to other networks. A network so organized is called a Public Land Mobile Network (PLMN). The mobile terminals connect to radio base stations via designated air channels. The base stations connect to the mobile network using leased lines. The core component in the PLMN is the Home Location Register (HLR) that contains all information about the subscribers in the network. The HLR is backed up by a set of Visiting Location Registers (VLR) to which the Mobile Switching Centers connect when deciding on if users are allowed to connect, make calls, etc..

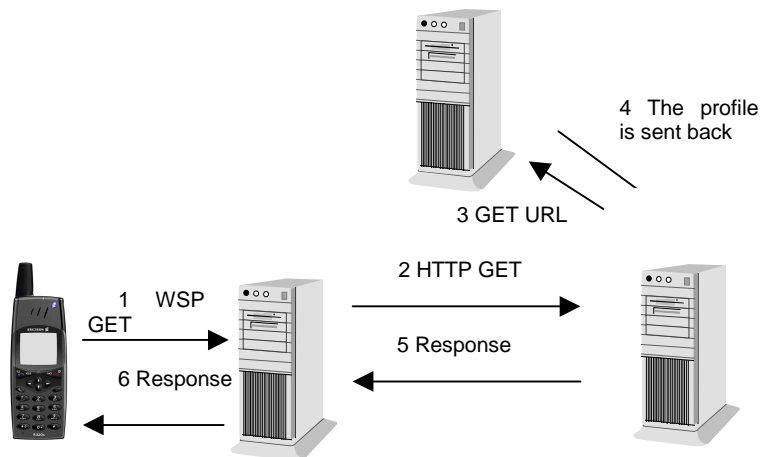
#### **3.2 WAP Application Architecture**

"The Wireless Application Protocol (WAP) is an open, global specification that empowers mobile users with mobile devices to easily access and interact with information and services instantly" [WAP]. It describes how to send requests and responses over a wireless connection, using the Wireless Session Protocol (WSP), which is an extended and bytecoded version of HTTP 1.1 [WSP]. Typically, a WSP request is sent from a mobile device to a WAP Gateway/Proxy (WAP Gateway), from where an HTTP session with the target web server is established [WBXML]. Over this session, the WSP request, converted into HTTP, is sent. The content, typically presented in the Wireless Mark-up Language (WML) is sent back to the WAP Gateway, where it is bytecoded and sent to the device over the WSP session.

#### **3.3 Composite Capabilities/Preferences Profiles (CC/PP)**

CC/PP is a framework for conveying capabilities and preferences associated with users and the user agents when accessing resources on the World Wide Web. CC/PP is intended to provide information necessary to adapt the content and the content delivery mechanisms to best fit the capabilities and preferences of the users and their web browsers.

CC/PP was published as a set of working drafts [CC/PP Req 2000] of the World Wide Web Consortium (W3C) in 2000. The User-Agent Profile (UAProf) Drafting Committee of the WAP Forum created a specification [UAProf] based on the original CC/PP note [CC/PP Note 1999] including some WAP specific extensions.



**Fig. 1.** CC/PP exchange as implemented in UAProf

CC/PP allows origin servers to generate content that is adapted to the requesting user-agent and the user's preferences by sending Capabilities and Preference Information (CPI) within an HTTP or WSP request to the origin server. CPI is represented by means of a profile, which comprises a set of components. In UAProf, these include hardware platform, software platform, network characteristics and personal settings. Each component is a placeholder for related attributes. The UAProf specification also defines location as a reserved attribute.

Profile Unified Resource Identifiers (URI) are sent using the profile header inside the HTTP request. The URI refers to the location of the profile. Intermediate network entities may optionally add content transforming capabilities or location information to the profile by adding a special header called Profile-diff, devoted to the purpose of conveying single or few attributes.

The example depicted in Fig. 2 shows how the CC/PP exchange protocol works in the UAProf scenario. Prerequisites for this example are that the user of the user equipment (UE) has initiated a WSP session with the WAP Gateway, and that in doing so, the device has used the appropriate mechanisms to convey one or more URI's pointing to where its profile components are stored. The profile information is then cached in the WAP Gateway.

In step 1, the user requests a resource located at an origin server as indicated by a web address (URL) included in a WSP request. In step 2, the WAP Gateway transforms the WSP request into an HTTP request, adding the profile URIs cached during WSP session initiation. In step 3, the origin server retrieves the CPI as indicated by the profile URIs from a profile repository. The origin server generates content adapted to the profile, and returns it (5) to the WAP Gateway, which performs any other necessary content transformation (if it supports it), including binary encoding of WML, and forwards the content (6) to the UE.

### 3.4 Location Based Services

Passing on the user's geographical location to the service provider opens up a whole range of new possible features [Hjelm et al. 2000], many on the theme "find the nearest...". Most developers of WAP related software today provide such a feature for telecom operators. With Global Positioning System (GPS) devices or such, it is not likely that operators will be the only service providers that will receive this kind of information.

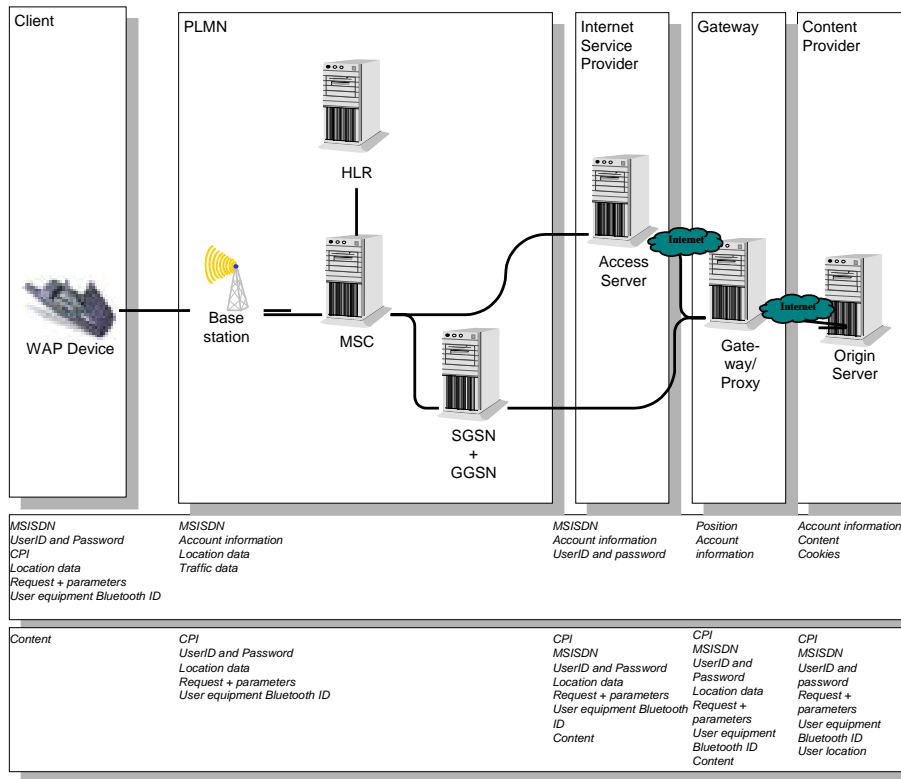
The methods for location passing vary. The following are possible:

- The device knows its own location, using GPS or some related technology, and passes it on with the request, e.g. by using the UAProf attribute or a proprietary HTTP header
- The operator of a PLMN/GSM network knows the user's location through base station information, and makes calculations from the strength of the signal within different cells, and:
  - adds the information to the request by having all requests pass a proxy, at the operator's location
  - provides an Application Programming Interface (API) for the service creator from where the location can be retrieved. There are components that the operator can install, from where the user's location can be redrawn. By providing application programmers with an API to this component, the location can be retrieved by the service when needed.

Especially for emergency services, precise location data are useful. However, while location based services offer great potentials for value added services, it is also necessary to ensure appropriate data protection and privacy safeguards.

## 4 Privacy risks in the mobile Internet

Fig. 2 shows an end-to-end WAP system, in an as generic way as possible. The upper five boxes are there to describe the environments where the components are usually found. The PLMN, Internet Service Provider, Gateway Holder and Content Provider can all be the same company, i.e. a network operator, but they can also be with separate organizations.



**Fig. 2.** An end-to-end WAP system

The upper horizontal box shows data that originates from or is normally stored in the environment described above.

The lower horizontal box shows data that can normally be captured as it passes by the environment.

#### 4.1 Exposed personal data

A side effect of global wireless communication is that traffic data and possibly further personal user characteristics that are transferred with messages, and also user data inside content, can be collected at different sites and used to create communication or user behavior profiles.

As shown in Fig. 2, the nodes in an end-to-end WAP system use, transfer and/or collect the following personal data items about users. The vertical rectangles show the different environments that the requests and responses pass through, the upper horizontal rectangle shows the data that originates from the node, and the lower the data that typically reaches this node from other components.

#### **4.1.1 The WAP Device**

The client device stores information such as the user's telephone number (usually the MSISDN number), user ID and passwords to the WAP Gateway and access server, and CPI profile information about the device's software and hardware characteristics, the network to which the device is connected and personal settings (see 3.2). It may have access to its geographic location by using for example the Global Positioning System (GPS), and it may also have a Bluetooth ID, which uniquely identifies the device.

When a request is being made, the URL, parameters and some or all of the information above will be sent with it to the Public Land Mobile Network (PLMN).

#### **4.1.2 Public Land Mobile Network**

There are a number of components inside the operator's environment [ETSI GSM 03.71] that the request will pass through. The operator holds information about the user's location and traffic data needed for transmission of a request. Traffic data is also processed to calculate accounting data for billing purposes.

If this information is combined with requests, parameters and content that pass the environment, and also CPI data, the operator can have a detailed profile of the user's activities. Generally, however, the routing in the PLMN is on a lower level, and advanced equipment is needed in order to unpack the information sent to and from the device. Also, encryption can be used protect against illegal interceptions. Besides, in contrast to origin servers and WAP Gateways that could be placed in non-trustworthy domains, operators are usually more able to handle private information, due to the fact that they normally risk heavy penalties otherwise. Most western countries have legal provisions, for instance for processing and storing traffic data.

Thus, in this paper, we do not address privacy risks in the operator's environment.

In Fig. 1, the traffic can take one out of two possible ways at the Mobile Switching Center, depending on whether or not a General Packet Radio Systems (GPRS) connection is used. In the first case, the traffic passes a Serving GPRS Support Node (SGSN) and a Gateway GPRS Support Node (GGSN), while if a circuit switched connection is used, an access server is needed.

#### **4.1.3 Access Server**

The access server is involved when we have a circuit switched connection. All the data that was mentioned above will at a worst case scenario be exposed to the holder of the access server, as it is possible to log what device connects to what gateway. If the traffic is not encrypted, all traffic data is also visible at this point. If this is an Internet Service Provider (ISP), account information may also be available, and possible to put together with the rest.

#### **4.1.4 WAP Gateway/Proxy**

The WAP Gateway can be placed either before the actual Internet connection, or at some Internet location, though the Internet does not need to be involved at all. The connection can be made directly to a secure area. WAP Gateway owners can be the

operator, the user's company if an intranet is provided, the service provider, especially if the data is particularly sensitive, such as for a bank, or and ISP.

Most WAP Gateway owners are likely to use subscriptions, which implies that the user will be identified when a request is made. The user will have a profile stored in the WAP Gateway, where history lists might be collected.

The WAP Gateway is the aggregation point of all requests. Since the WAP Gateway unpacks all the layers in the stack, the requests, parameters and content together with CPI, location data and other user identifying data can easily be seen here. Since the user usually only uses one or a small number of WAP Gateways, such personal information related with all requests of a user can be aggregated at the WAP Gateway. This makes the WAP Gateway, together with the origin servers, the critical components from a privacy perspective.

WAP gateways are often used as anonymizers, to filter out personal data, such as the MSISDN number. By enforcing the use of multiple gateways, i.e. the user changes gateways for specific applications, or in given time intervals, the level of privacy can be enhanced. A different view on the use of gateways is given in section 5.3.

#### **4.1.5 Origin Server**

The origin server can be located either in immediate connection with the WAP Gateway, or somewhere on the Internet. In both cases, the user's identity can be revealed without the user's knowledge – either by having the origin server and the WAP Gateway share the same user database, or by passing the identity of the user with the request. In many countries, passing the user's phone number (MSISDN) with the request is not allowed outside the operator's environment. However, the operator might extend its environment to include other service providers. Even if user ID forwarding is not used, a web page logon is required for some applications, where the user's identity and address are requested, for instance to deliver ordered goods.

Besides the requests, parameters, CPI, location data and other user identifying data that are forwarded by the WAP Gateway to the origin server, the origin server site can also post cookies and can store session data (time, type of transaction) and data about transferred files.

Origin servers might be placed in countries without or with no stringent privacy legislation and it is often unclear how far they can be trusted to respect the user's privacy.

## **4.2 Misuse Scenarios**

Particularly at the WAP Gateway and origin server's site, various personal characteristics about the users are available that can be used to trace their requests, interests, habits, preferences, movements and to aggregate such information in extensive personal profiles.

In principle, all personal data can be sensitive dependent on the purpose of their use. This also holds for user device-specific CPI, which can contain detailed characteristics about a user's device hardware, software, used network and personal settings and can be unique for a specific user with a specific device. The CPI can serve as a unique identifier and can, like a user ID, be used to trace a user's request

activities at the origin server's site. Furthermore, CPI can tell what device, software, settings or network a user is using.

In the misuse scenarios below, we introduce wickedsite.com. At that site, the owner collects all possible information about the user, such as name, address, selected password, MSISDN and Capability Preferences Information. The owner has many friends, and has never discovered nor cared about privacy.

#### **4.2.1 Social Engineering Attack Scenario**

Money Penny often uses "wickedsite.com". From her provided information, the operator of the site can perform a social engineering attack [Winkler et al. 1995] on her employer. One way is to call the user, if the phone number (MSISDN) has been provided to that site, and ask where she works by saying "Have I reached company ...?", and hopefully get the answer "No, this is company ..." back. This information gives the target of the attack. By trying the user ID and password selected by the user at "wickedsite.com", or by using the same methods as described in [Winkler et al. 1995] to retrieve the user ID, an attack can be performed on the user's company.

#### **4.2.2 The Location Scenario**

There are many ways to use location information for malicious purposes. Here is one simple example (see also [Hjelm et al. 2000]).

Lady and the Tramp, who frequently use location-based services at wickedsite.com, have a relationship that they wish should remain unknown. Since the wife of the Tramp has hired a detective, who also knows the owners of the site, he can easily first tie both of them together historically, and then find out where they are at a specific moment, and be there with his camera.

#### **4.2.3 The Disability Scenario**

As described in [CC/PP Note 1999], the profile information set in the device can be extended into comprising almost anything. Assume there is a setting saying the user can ask for larger letters and no images. From this information, conclusions can be drawn.

Minnie has eye disabilities, and, in order to get adapted information, she has made this setting in her device. When she applies for a new job, her potential employer finds this out by asking the owners of wickedsite.com.

#### **4.2.4 The Illiterate People Scenario**

Using the same information as described in the scenario above, a company in a developing country finds out who of his customers are illiterate by looking at the "No Text" setting, finds them through the MSISDN number or provided address and uses this information to trick them or bribe them.

#### **4.2.5 The Expensive Phone Scenario**

Simon has recently bought a new, expensive phone, from money that his grandmother provided him with in her will. This information can be used by attackers looking for wealthy "targets" suitable for a break-in.

## 5 Privacy Enhancements

There are different ways of enhancing privacy in the mobile Internet by technology. One is to eliminate or minimize the data that can be read by the owners of the components in the network, and another is to technically control that personal data are only used according to legal provisions or agreements with the user. Below, P3P will be briefly introduced and it will be discussed how P3P can be used to enforce user control over personal or device-related data by allowing to forward such data only if there is an informed consent by the user. Further privacy-enhancing mechanisms for anonymizing requests or hiding personal data to passing components will only be briefly addressed in the next section.

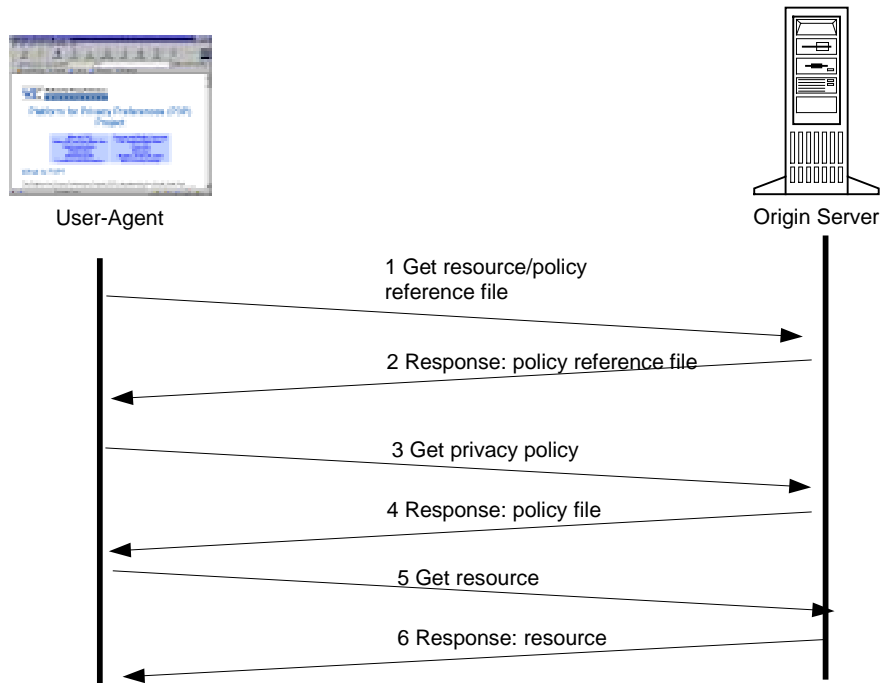
### 5.1 The Platform for Privacy Preferences (P3P)

The W3C P3P [P3P] candidate recommendation specifies a protocol that provides an automated way for users to gain more control over the use of personal data on web sites they visit. P3P enables Web sites to express their privacy practices in a machine-readable XML format that can be retrieved automatically, interpreted easily and compared with the user's privacy preferences by user agents. Using this information, the user can make informed decisions on whether or not to submit a certain piece of personal information to the Web site.

It is possible to cover the entire web site with one privacy policy or to use different policies for different parts of the web site (e.g., in an electronic shopping mall, different shops might have different policies). A policy reference file is used to associate P3P policies with certain regions of URI-space.

The location of the policy reference file can be indicated using one of three mechanisms:

- Well-known location at the web site (`/w3c/p3p.xml`).
- Reference through an HTTP header: the HTTP response includes a URI in a header pointing to the policy reference file.
- Inclusion in the result: the privacy policy reference URI may be included as a part of the actual content using the link tag.



**Fig. 3.** The P3P agreement

The following example explains how P3P works, when a client retrieves a document, which in its turn asks the user for information, e.g. her phone number.

As depicted in Fig. 3, P3P comprises six steps. In step 1, the user agent asks for a resource/ policy reference file available at an origin server. The Web server responds back to the device, in step 2, by sending the policy reference file. In step 3, the user-agent requests the privacy policy, the origin server returns the file in step 4. The user agent compares the site's privacy policy with the user's privacy preferences, and authorizes the release of personal data only if the user's preferences as well as the requested data transfer are consistent with the policy. Assuming that this is the case, in step 5, the user-agent issues a request to retrieve the resource the user wants and in step 6, the page is returned to the requesting user agent.

The communication for fetching the policy reference file and the privacy policies should be part of a special so-called "safe zone", in which minimal data collection takes place and any data that is collected is used in only non-identifiable way. In particular, user agents should not send HTTP Referer headers or accept cookies in the safe zone.

## 5.2 Protecting CPI with P3P

In order to protect the user's right for informational self-determination, users should have control over the CPI of their devices, and determine themselves how far and to what extent they want to communicate profile information to other sites.

The CC/PP working group has expressed the design goal that the Platform for Privacy Preferences (P3P) is to be used as a management mechanism for the privacy of profiles. P3P can enhance the user's privacy by transmitting CPI (and possibly other personal characteristics, such as location data – unless already included as an CPI attribute) only if there is an informed consent by the user about the origin server's site data collection and use practices (how and for what purpose CPI will be used, with whom data will be shared, how long the data will be retained).

However, with the CC/PP exchange protocol, a user uses a modified WSP or HTTP GET request which already carries the profile information or profile difference, whereas according to the P3P standard, it is first checked whether there is a sufficient match between a user's privacy preferences and the remote server's privacy policy before any personal data is transmitted.

Thus, in order to use CC/PP with the P3P standard, it is first required that the user defines a minimal profile with only minimal CPI. This minimal profile should include only such CPI (such as for instance screen size, voice or graphic capabilities) that the user is ready to reveal even to sites with whom the user has not come to a P3P agreement so far. In the extreme case in which the user does not want to provide any information to possibly non-trustworthy sites, the user could define that the minimal profile be empty.

Thus, the minimal profile can be used

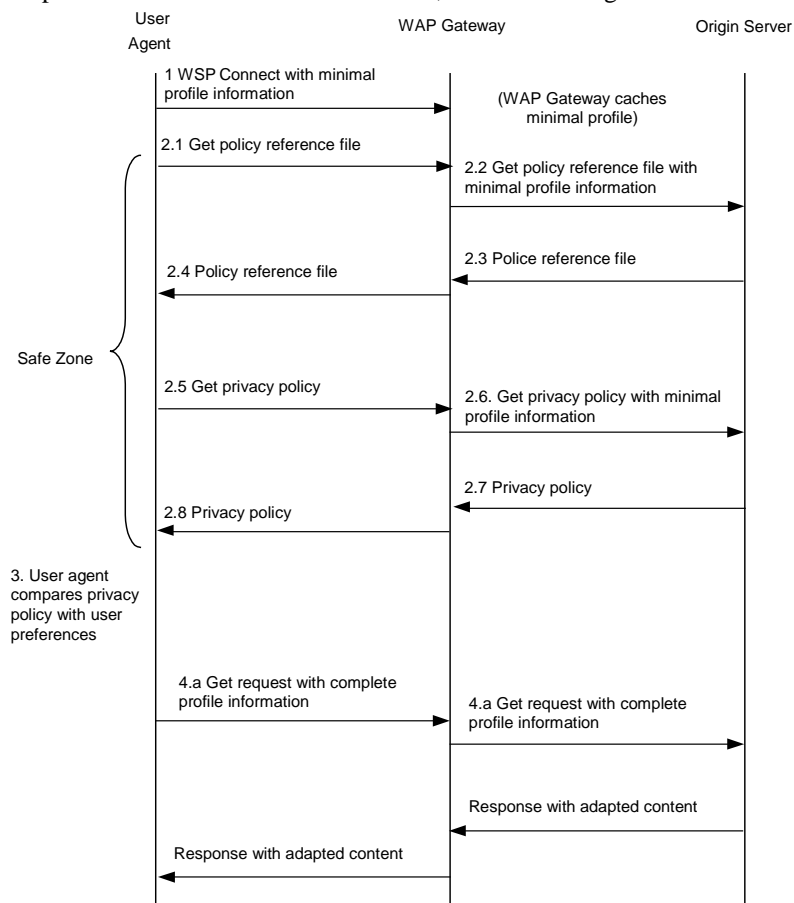
- for communication in the “safe-zone” before a P3P agreement;
- for accessing non-P3P enabled web sites or web sites that do not meet the user's P3P privacy preferences;
- and optionally for serving third party requests to the WAP Gateway for cached profiles (for instance, to generate content that will subsequently be pushed to the client device)

The following use case describes the steps of communication for the case where the user has defined a minimal profile and the P3P protocol is used to agree about the data collection and use of further CPI:

1. Upon opening a WSP session, the client conveys its minimal profile information using Profile and Profile-Diff headers within the WSP Connect request. The WAP Gateway caches the minimal profile for the lifetime of the session.
2. If the user wants to request content from a P3P enabled site, she first requests the site's P3P policy reference file by issuing a standard WSP request to the WAP Gateway. The WAP Gateway forwards the request via HTTP including the user's minimal CPI associated with the session. After having received the policy reference file, the user requests the privacy policy in the same manner. Thus, for the communication in the safe zone, only the minimal profile is forwarded by the WAP Gateway to the origin server.
3. The user agent compares the site's privacy policy with the user's preferences to determine whether further CPI should be transmitted. Users should have the

possibility to choose the level of protection by defining privacy preferences for the whole CPI, or different preferences for CPI components and/or attributes.

4. If the user or her agent accepts the origin server site's privacy policy, there are different options of how further CPI can be transmitted to the origin server:
  - a. To augment the minimal profile, the client includes profile and/or profile-diff headers with each subsequent WSP request in that session as depicted in Fig. 4. The WAP Gateway then overrides the cached minimal profile with the provided headers, when it generates an HTTP request.
  - b. The user sends a WSP session Resume message to the WAP Gateway containing profile and/or profile-diff headers with the new CPI and the WAP Gateway will update the cached CPI for that session, as shown in Fig. 5.



**Fig. 4.** The complete CPI is conveyed with every WSP request issued after the P3P agreement

Also, if the user agrees that certain CPI attributes (e.g., the user location) might be augmented by the WAP Gateway, the WSP requests or resume message should have a flag/attribute set that authorizes the WAP Gateway to add that information to the CPI.

Sending the complete profile information with each subsequent request has the advantage that the complete CPI profile of user device will not be cached in the WAP Gateway. However, in contrast to option 4.b, also CPI, and thus more data, has to be transferred with each request. Option 4.b can only be used if one privacy policy is valid for an entire Web site.

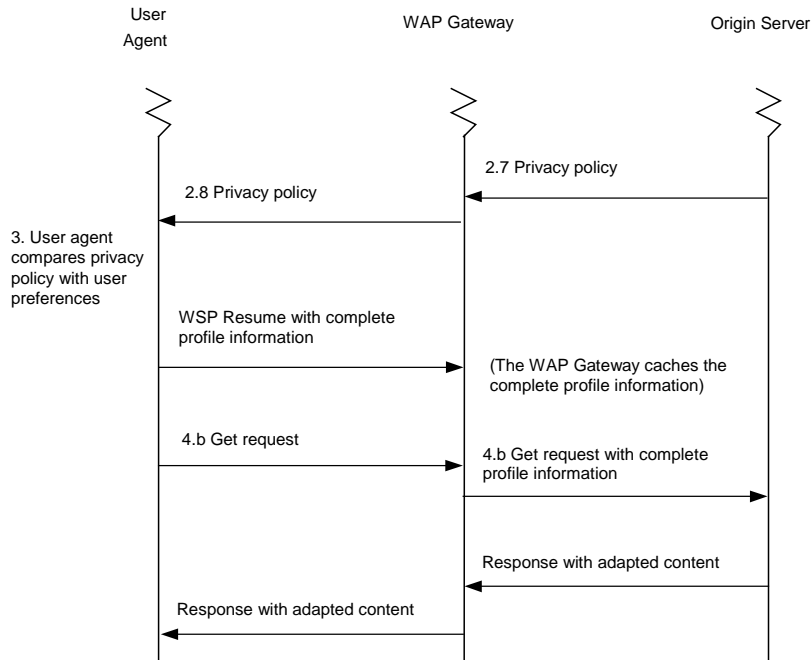


Fig. 5. The complete CPI is sent with the WSP Resume after the P3P agreement

### 5.3 A Trust Relationship between the User and the WAP Gateway

The P3P protocol can be used to inform mobile users about the data-collection and data-use practices (P3P policy) of the origin server site and to help users to reach a semi-automated agreement with the site with regard to the processing of an individual's personal data. However, besides the origin server site also the WAP Gateway as an intermediary receives the CPI. The WAP Gateway caches the CPI for a session and may also use profile information to transform the encoding format of content. Also, the WAP Gateway may optionally augment the received CPI with additional data obtained from local databases, such as location data from the operator's network. Thus, it is crucial that the user can also set up a trust relationship with the WAP Gateways she uses. Usually, the user uses one WAP Gateway that belongs either to the operator or user domain. Furthermore, for applications with high

security requirements (e.g., bank applications), a WAP Gateway could be also placed in the origin server's domain.

Thus, the set of WAP Gateways that a user is using is small and does not vary much. The user can usually know what WAP Gateways are used as intermediaries beforehand. Hence, a simple way to set up a trust relationship could be as follow:

1. Each WAP Gateway publishes its privacy policy with a validity period. Such a privacy policy should consider basic privacy requirements, such as necessity of data collection and purpose binding. In particular, WAP Gateways should only use personal user data for the purpose of encoding and forwarding to the requested origin servers. They should only store personal user data for the duration of a session and keep it confidential.
2. Users can view and accept the WAP Gateway's privacy policy before they decide to use that WAP Gateway. The user device can store a list of trusted WAP Gateways of the form (ID of accepted WAP Gateway, validity period), where the combination of the phone number of an access server plus the IP address of the WAP Gateway could serve as a unique ID for the WAP Gateway. Only WAP Gateways from that list will be contacted.

#### **5.4 Enhancements of P3P and its Operation Environment**

As discussed above, P3P can enhance the user's privacy by informing her about a web site's privacy practices and letting the user decide in dependence of that privacy policy what personal data for what purposes she wants to reveal. Nevertheless, P3P has several weaknesses and limitations (see also [EPIC 2000]):

First of all, P3P does not provide a technical mechanism for making sure that sites only ask for personal information as far as necessary and that sites act according to their policies. Hence, whereas P3P can implement informed consent, it does not support other essential provisions of the EU-Directive, such as Art.6b (purpose binding), Art.6c, Art.7 (necessity of data collection and processing) and Art.12 (right of access). Thus P3P alone is not a sufficient solution. Privacy advocates have actually even expressed their concerns that P3P can in practice be used to push users to give up their privacy by forcing them to reveal more personal data than necessary in exchange to the provision of a service.

According to German Multimedia Legislation (§3 (3) Teleservices Data Protection Act – TDDSG), the service provider may not make the use of services conditional upon the consent of the user to the effect that this data may be processed or used for other purposes than necessary, if other access to these services is not reasonably provided to the users. Corresponding regulations should be established at international level.

A next step within our research project is to work on a proposal how P3P and other security mechanisms can be combined to support the implementation of basic privacy requirements of the EU data protection Directive at the web server's site:

Within a former research project, a formal privacy model has been developed and implemented according the Generalized Framework of Access Control- Approach in the Linux system kernel [Fischer-Hübner / Ott 1998], [Fischer-Hübner 2001]. The privacy model was designed as a security model that can technically enforce legal

privacy requirements such as purpose restriction and necessity of data processing. It is planned to adapt the privacy model implementation, so that it can be used in combination with third party monitoring and assurance to protect P3P data elements at the server's site in order to ensure that personal data elements are collected and processed only as far as necessary and only used for the specified purposes.

Another problem is that P3P is an inherently "chatty" protocol. When used over wireless links, it creates much round-trip time, as extra round trips are required to fetch the privacy reference file and the privacy policies. According to earlier P3P specifications, if there is a match between the site's privacy policy and the user's preferences, the user agent would send an acceptance notification identified by a pairwise or site ID (PUID) which is unique to every agreement the agent reaches with the service. When the user accesses the web site the next time, the user agent can forward the PUID to indicate that the site's privacy policy already matched the user's preferences. Thus, such a P3P extension could help to save valuable roundtrip time.

## **5.5 Data Hiding, Minimization and Avoidance**

By hiding, encrypting, minimizing or even avoiding personal data, the risks of data collection along the way to the origin server will decrease.

Kudo and Hada [Kudo et al. 2000] propose a way to integrate security features such as non-repudiation, confidentiality and authorization through an XML access control language, which includes both a specification for encryption on the application layer, derived from [XML Signature 2000], and an architecture for access methods. Obviously, application layer encryption can hide content from components other than the intended recipient. This can be used in combination with for example P3P.

Several parts of the transformation is already hidden through lower layer encryption. First, GSM encryption (if actually provided by the GSM network) is automatically used. Also, the Wireless Transport Layer Security (WTLS) protocol can be used to establish a secure link between the user device and the WAP gateway, and from the gateway to the origin server, Secure Session Layer (SSL) or such could be used. This, however, will not hide any data from the WAP gateway, since all the layers are unpacked there.

As discussed in section 4, WAP Gateways receive, translate and forward all requests telling who requests what using what device and thus can easily create extensive personal user profiles. Hence, also privacy-enhanced system concepts are needed to protect user identities at the WAP Gateway site. The use of privacy-enhancing technologies such as for instance Mix nets for providing anonymity at the WAP Gateway site should be examined. A Mix net introduced by D. Chaum [Chaum 1981] can realize unlinkability of sender and recipient as well as sender anonymity against the recipient. If a request would be send through a mix net to the WAP Gateway, the user identity could be hidden from the gateway. Onion Routing [Syverson et al. 1997] and the Freedom Network [Freedom 2000] are practical examples of network architectures that apply the mix concept to provide anonymous interactive Internet communication.

Another way of ensuring a degree of anonymity whereby the user appears to be no more likely than not to be the initiator of a given transaction is presented in [Shields et al 2000]. The named solution combines a set of proxies with multicast routing, the result is proven to be both more efficient and more secure than other solutions, specifically onion routing [Syverson et al. 1997] and Crowds [Reiter et al 1998].

Similar architectures for providing anonymity of communication should also be developed for the mobile Internet.

## 6 Conclusions and Outlook

In this paper, we have shown that the user's privacy is at risk in the mobile Internet. Personal data, such as traffic data, location data, CPI and content data is available at different sites. The mobile Internet may fail to gain consumer acceptance because of fundamental privacy problems. To protect privacy, a holistic approach is needed including legal means, privacy-enhancing technologies as well as educational measures for raising awareness and teaching users how to apply privacy-enhancing technologies.

Legal privacy requirements for the mobile Internet environment were recently formulated in the Proposal for an EU Directive concerning the processing of personal data and the protection of privacy in the electronic communication sector [EU Directive-Proposal 2000]. The proposed directive addresses also the protection of location data and requires that location data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service.

In this paper, we have further suggested and discussed some technical solutions for enhancing privacy in the mobile Internet. We showed how the P3P protocol could be used to enforce user control over CPI including location data, allowing the transfer of CPI and location data only if there is an informed consent of the user. Thus, the P3P protocol can be used to protect location data according to the requirement of the EU directive proposal. A further step in our research project will be the implementation and testing of a P3P-compliant WAP browser that acts according to the protocol specified in section 5.2. Besides, as mentioned above, we will work on the adaptation of a privacy access control model to protect personal data exchanged in a P3P agreement at the origin server's site. Furthermore, we plan to examine how anonymous communication can be implemented in the mobile Internet.

**Acknowledgements:** Part of this work has been funded by the HumanIT research programme at Karlstad University. We therefore want to thank HumanIT for their support. We also thank the referees for helpful comments.

## References

- [CC/PP Req 2000] M. Nilsson, J. Hjelm, H. Ohto. CC/PP: Requirements and Architecture. *W3C Working Draft*. URL: <http://www.w3.org/TR/2000/WD-CCPP-ra-20000721/>. July 2000.
- [CC/PP Note 1999] F. Reynolds, J. Hjelm, S. Dawkins, S. Singhal. CC/PP: A user side framework for content negotiation. *W3C Note*, URL: <http://www.w3.org/TR/NOTE-CCPP/>. July 1999.
- [Chaum 1981] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", *Communications of the ACM*, 24 (2). 1981, pp. 84-88, <http://world.std.com/~franl/crypto/chaum-acm-1981.html>
- [EPIC 2000] Electronic Privacy Information Center (EPIC), Pretty Poor Privacy: An Assessment of P3P and Internet Privacy. URL: <http://www.epic.org/reports/prettypoorprivacy.html>. June 2000.
- [ETSI GSM 03.71] ETSI Specification GSM 03.71 V7.3.0. *ETSI Technical Specification GSM 03.71*. February 2000.
- [EU Directive 1995] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, <http://europa.eu.int/ISPO/legal/en/dataprot/directiv/directiv.html>
- [EU Directive-Proposal 2000] Proposal for a Directive of the European Parliament and of the Council. *Commission of the European Communities*. COM(2000) 385. July 2000. [http://europa.eu.int/comm/information\\_society/policy/framework/pdf/com2000385\\_en.pdf](http://europa.eu.int/comm/information_society/policy/framework/pdf/com2000385_en.pdf)
- [EU Telecommunication Directive 1997] Directive 97/66/EC of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector of 15 December 1997.
- [Fischer-Hübner et al. 1998] Simone Fischer-Hübner, Amon Ott., From a Formal Privacy Model to its Implementation. Proceedings of the 21st National Information Systems Security Conference. Arlington, VA. October 5-8, 1998.
- [Fischer-Hübner 2000] Simone Fischer-Hübner. Privacy and Security at Risk in the Global Information Society. in: D. Thomas, B. Loader (Eds.): *Cybercrime*. Routledge. London and New York, 2000.
- [Fischer-Hübner 2001] Simone Fischer-Hübner. IT Security and Privacy - Design and use of Privacy-enhancing Security Mechanisms, Springer, Lecture Notes in Computer Science, LNCS 1958, May 2001.
- [Freedom 2000] Philippe Boucher, Adam Shostack, Ian Goldberg, "Freedom System 2.0 Architecture, White Paper, Zeroknowledge Systems, 2000. <http://www.freedom.net/info/freedompapers/index.html>
- [Hjelm et al. 2000] J. Hjelm, M. Nilsson. Position dependent services using metadata profile matching. *iNet, the Internet Society Conference*. URL: <http://www.wireless-information.net/Johan/Engelska/inet00-paper-01.htm>. July 2000.
- [Kudo et al. 2000] M. Kudo, S. Hada. XML Document Security based on Provisional Authorization. *Proceedings of the 7<sup>th</sup> ACM Conference on Computer and Communication Security*, pages 87-96. November 2000.
- [OECD 1980] Organisation for Economic Cooperation and Development - Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 23<sup>rd</sup> September 1980.
- [P3P] *Platform for Privacy Preferences (P3P)*. URL: <http://www.w3.org/P3P>.
- [Reiter et al. 1998] M.K. Reiter and A.D. Rubin. Crowds: Anonymity for Web Transactions. *ACM Transactions on Information and System Security*, 1(1):66-92, November 1998.

- [Shields et al. 2000] C. Shields and B. N. Levine. A Protocol for Anonymous Communication Over the Internet. *Proceedings of the 7<sup>th</sup> ACM Conference on Computer and Communications Security*, pages 33-42. November 2000.
- [Syverson et al. 1997] P. Syverson, D. Goldschlag, M. Reed, "Anonymous Connections and Onion Routing", Proceedings of the 1997 Symposium on Security and Privacy, Oakland, 1997, <http://www.onion-router.net/Publications.html>
- [UAPProf] WAP-174: WAG UAPROF User Agent Profile Specification. Wireless Application Group. <http://www1.wapforum.org/tech/terms.asp?doc=SPEC-UAPProf-19991110.pdf>
- [WAP] The Wireless Application Protocol Forum. <http://www.wapforum.org/>
- [WBXML] WAP-192: WAP Binary XML Content Format. WAP Forum. URL: <http://www1.wapforum.org/tech/terms.asp?doc=WAP-192-WBXML-20000306-a.pdf>. May 2000.
- [Westin 1967] Alan Westin. Privacy and Freedom. New York. 1967.
- [Winkler et al. 1995] I. Winkler, B Dealy. A Case Study in Social Engineering. *Proceedings of the 5<sup>th</sup> ACM Conference on Computer and Communications Security* June 1995.
- [WSP] "Wireless Application Protocol, Wireless Session Protocol Specification", WAP-203-WSP, WAP Forum, 4-May-2000. URL: <http://www.wapforum.org>
- [XML Signature 2000] M Bartel, J Boyer, B Fox, E Simon. XML-Signature Syntax and Processing. *W3C Candidate Recommendation 31*. October 2000.