30

SELF-DETERMINATION IN MOBILE INTERNET

PiMI Prototype Results

Simone Fischer-Hübner[1], Mikael Nilsson[2], and Helena Lindskog[2]
[1]*Karlstad University, Department of Computer Science, SE-651 88 Karlstad, Sweden*
[2] *Ericsson, Box 1038, SE-651 15 Karlstad, Sweden*
simone.fischer-huebner@kau.se, {mikael.nilsson, helena.lindskog}@ericsson.com

Abstract: Mobile Internet environments will offer a whole new range of services that might revolutionize our way of life. However, with these new technologies and services new risks to the user's privacy arise, and both legal and technical privacy safeguards are needed to protect the user. This paper discusses privacy and privacy risks in the mobile Internet and presents the result of the PiMI prototype project, in which one browser built-in, and one proxy-based P3P user agent for mobile Internet environments have been developed. The PiMI prototype enhances the users' control over the dissemination of user and user-device related information and thus protects their right for informational self-determination.

Key words: mobile Internet, privacy, profiles, UAProf, CC/PP, P3P, WAP, privacy-enhancing technologies

1. INTRODUCTION

The mobile Internet promises applications featuring rich content, comprising text, audio and streaming video in full color. The range of possible services that can be developed using these features together with the unique characteristics of mobile networks is immense.

The mobile Internet allows users to access traditional Internet services and other server-based applications from mobile devices, and also makes new services possible, such as location-based and context-aware applications. The CC/PP [CC/PP] exchange protocol conveys capability and preference information (CPI) when accessing Web resources to ease content adaptation to best fit the capabilities and preferences of the user agents and users. While mobile services can be of great use, privacy risks need to be considered as well. With these new protocols or services, personal data such as lo-

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35586-3_46

M. A. Ghonaimy et al. (eds.), *Security in the Information Society*

cation data, CPI and further user attributes are transferred with messages and exposed at different nodes, such as the WAP gateway/proxy or the Origin Server's site. Appropriate legal and technical data protection and privacy safeguards must be implemented. Mobile Internet users must not be under permanent surveillance, or they might not use any mobile Internet services all.

At Karlstad University, we have investigated privacy and privacy risks in the mobile Internet, as well as technical means for enhancing the user's privacy, in cooperation with Ericsson. Particularly, we have analyzed how the Platform for Privacy Preferences Project (P3P) protocol can be used to enforce the user's control over the release of CPI and location data (see also [Nilsson et al. 2001]). In the PiMI ("Privacy in Mobile Internet") prototype project at Ericsson, a browser built-in and a proxy-based P3P user agent for mobile Internet environments have been developed.

This paper presents the results of the PiMI prototype project. In section 2, privacy and basic privacy requirements are described. In section 3, we briefly explain the mobile Internet architecture. Privacy risks in mobile Internet environments are discussed in section 4, followed by Privacy-Enhancing Technologies and the Platform for Privacy Preference Project (P3P) in section 5. Section 6 describes the results from the PiMI prototype project, and section 7 concludes the paper. We have investigated problems and solutions in WAP systems, but the same ideas will hold for other mobile Internet architectures.

2. PRIVACY

Privacy is well recognized as a fundamental human right. In general the concept of privacy has three aspects [Rosenberg 1992], [Holvast 1993]:

- **Privacy of the person** - by protecting a person against undue interference, such as physical searches or information violating his moral sense
- **Territorial privacy** - by protecting the close physical area surrounding a person
- **Informational privacy** - by controlling whether and how personal data can be gathered, stored, processed or selectively disseminated

The most common definition of informational 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, which according to Westin and other common definitions can be defined as the right of informational self-determination. In order to pro-

tect this right, 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 the principles of legitimacy (personal data collection and processing is only admissible if permitted by legal provisions or if the data subject has consented, see Art. 7), purpose specification and purpose binding (see Art. 6), necessity of data collection and processing (see Art. 7), rights of the data subjects (see Art. 10 - 14), supervision and sanctions (see Art. 28), and adequate technical and organizational security safeguards (see Art17).

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].

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 (Art.10) and for necessary measures to safeguard security, defense and crime investigations (Art. 15).

3. MOBILE INTERNET ARCHITECTURE AND SERVICES

3.1 WAP 2.1 Architecture

"The Wireless Application Protocol (WAP) is an open, global specification that empowers mobile users with wireless devices to easily access and interact with information and services instantly" [WAP]. The version used in current products is 1.2.1. 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.

3.2 WAP 2.0

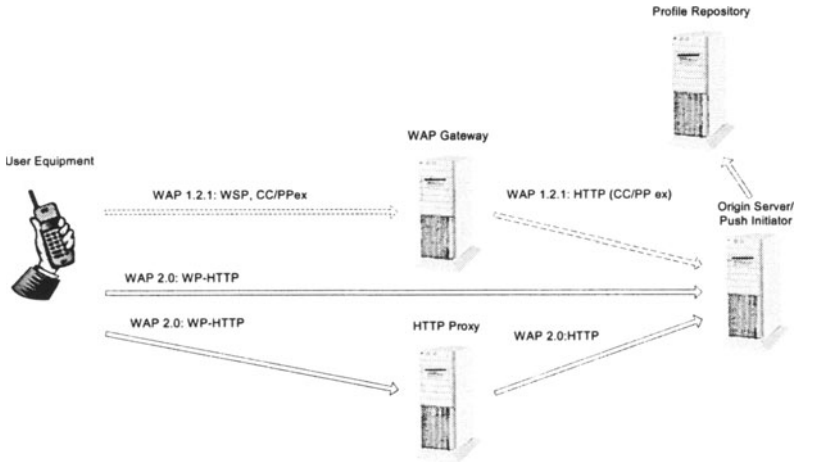

Figure 1. WAP 1.2.1 and WAP 2.0 programming models

The latest version of WAP to be released in the first quarter of 2002 relies on similar components as in WAP 1.2.1. The main difference is that the user equipment (UE) communicates with the origin server via a feature enhancing proxy directly over HTTP, as shown in Figure 1. The protocol stack in the mobile device is a Wireless Profiled (WP) TCP/IP stack. An important difference is that the use of a proxy/gateway now is optional, which means that the UE can issue HTTP requests over TCP/IP directly to the origin server, with no intermediaries.

On the application layer, the use of WML-specific extensions has been made optional. The WAP Forum standard XHTML Mobile Profile - a derivative of XHTML replaces WML as the mark-up language. This means that mobile devices now can access a large portion of legacy, non XML-

based HTML web sites directly, with no need for content translation or transcoding.

3.3 Personal Trusted Devices

The vision of the largest mobile device manufacturers, Ericsson, Nokia and Motorola and other companies in the industry [MeT Overview] is to broaden the role of the mobile phone. The device might be used for identification, authorization, payment and ticket storage and validation. This implies storage of private keys, certificates, credit card numbers, and identity units, typically stored in the subscriber identity module (SIM) card. Mechanisms for signing and a Bluetooth connection or similar are also needed. The MeT initiative implements these ideas [MeT Overview].

3.4 User-Agent Profiles

Composite Capabilities/Preferences Profile (CC/PP) [CC/PP] by the World Wide Web Consortium (W3C), specifies how a client side user-agent, such as a web browser in a PC, or a mobile phone, can deliver a description of its capabilities and the users' settings to an origin server. This is done so that an application on the origin server can generate content tailored to the characteristics and Man-Machine Interface (MMI) of the requesting device, and thus enhance the user experience and minimize the use of bandwidth.

CC/PP is defined as an application of the meta-data framework Resource Description Framework (RDF), which is in turn an XML application.

What is required by CC/PP, is that the description is done using a vocabulary. This results in a Capabilities and Preference Information (CPI) profile. This XML document comprises a set of components, within which attributes describing the user-agent and device reside. It is expected, that users of CC/PP define a vocabulary pertinent to their specific application.

CC/PP ex is a protocol defined for transmitting CPI over HTTP. It uses the HTTP extension framework, which is a mechanism that allows you to define new protocols on top of HTTP.

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.

The information sent with CC/PP can be divided into three categories:

- Device information (i.e. which device you are using and its capabilities) and network characteristics
- User settings (i.e. some preferences of the user)
- User information (prestored user information, or other context-dependent information, such as location)

3.5 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 a proprietary HTTP header, or the attributes available in UAProf, which can be used by the mobile device for conveying location information to origin servers
- 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

3.6 Context-Aware Services

A context-aware service is an internet service knowledgeable about the environment in which it and its user operates. Schilit [Schilit 1995] has defined context-aware services: "Application adaptation triggered by such things as the location of use, the collection of nearby people, the presence of accessible devices and other kinds of objects, as well as changes to all these things over time."

The concept of context awareness includes a lot of parameters, which can be divided into the major types activity, identity, location and time.

The data required to implement context-aware services can be collected in several different ways in a mobile network. Parlay [3GPP] provides a CORBA interface to SS7, SMS [ETSI GSM 03.37] provides a text based interface to SS7 and location information as data can be sent to/from clients in a generic way. Finally, standard/non-standard HTTP headers can be used to submit information to an application server.

4. PRIVACY RISKS

4.1 Risks Factors

Privacy in mobile Internet environments is much greater an issue than privacy in traditional Internet environments, due to the following four issues:

1. **The small screens**
   The fact that devices have smaller screens gives that personalization is much bigger an issue in the mobile Internet than in traditional

Internet environments, where personalization of sites is a matter of convenience to the end user. Personalization implies behavior tracking and profiling through log files, user databases or cookies, and also user settings. In a mobile Internet environment, surfing will hardly be worthwhile if you cannot retrieve the information that you wish in a few clicks.

2. **The wireless connection to the Internet**
   There are mainly two kinds of wireless connections:
   - **digital cellular systems, e.g. GSM**
     When using a digital cellular system, the telecom operator already knows your whereabouts. The mobile Internet does not today bring the possibility of tracking end users through IP numbers and traceroute commands, but there is a possibility that we will see such scenarios in the future.
   - **short-range radio links, e.g. Bluetooth**
     When using short-range radio links, the user is exposed to a new group of service providers, that are not as acquainted to handling personal information, e.g. shop owners or public transportation providers.
     In this case, there is also a new kind of territorial privacy threats, see section 2. In other words, a Bluetooth mobile Internet service provider, such as a train company or a retailer, can collect information about the end user, when the end user is close to the provider's Bluetooth access points, and then reuse this information to send personalized, and possibly unwanted, messages to the end user.
3. **The portability**
   The possibility to carry the device with you everywhere you go gives you a whole new range of possible services. Many of those require your position, in X and Y coordinates, but some might trigger on other things, such as the room that you just entered, see 3.6, or the fact that you are physically close to another person, and so on. A personal trusted device, see section 3.3, will provide you with the possibility to use your device instead of identity cards, credit cards or bonus cards.
4. **The difference in device capabilities**
   When requesting a URL within a traditional Internet environment, the device information that is normally transmitted over HTTP 1.1 [RFC 2068] is only the user-agent. Since most people use the MS Internet Explorer or Netscape browsers, this information tells little about the user. However, with user agent profiles of small devices,

much more information about the end user will be transmitted, see [UAProf].

4.2 Exposed Data

As discussed in [Nilsson et al. 2001], a side-effect of mobile Internet communication is that traffic data, location data, user preferences user or device characteristics that are transferred with a message as well as content data are exposed at different nodes and can be used to create communication profiles.

There are a number of components inside the operator's environment that the request will pass through. The operator holds information about the user's location and traffic data needed for transmission of a request. However, 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. Furthermore, most western countries have legal provisions, for instance for processing and storing traffic data.

In WAP 1.x systems, 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 capability and preference information (CPI), location data and other user-identifying data (Bluetooth ID, MSISDN) can easily be seen here. As 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. Although WAP gateways are often used as anonymizers to filter out personal data such as the MSISDN number, their profiling capability makes them, together with the origin servers, the critical components from a privacy perspective.

Personal user data can also be accumulated at the origin server's site. Besides the requests, parameters, CPI, location data and other user identifying data that are forwarded by the WAP Gateway to the origin server or requested by the origin server (in case of web page logon), the origin server site can also post cookies and 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.

As pointed out in [Nilsson et al. 2001], all exposed personal data can be sensitive dependent on the context and the purpose of their use. It is quite obvious that collecting location data and thus tracing the user's location is a severe privacy threat. However, also information such as about the device capabilities and user's preferences can become very sensitive if used in a certain context. For instance, the user's voice and graphic settings can reveal information about a user's eyes or ears (dis)abilities. Also the information

that a user owns an expensive mobile phone, could be misused by malicious attackers.

5. PRIVACY-ENHANCING TECHNOLOGIES

5.1 Basic Concepts

There are two major ways of enhancing privacy in the mobile Internet by technology. Privacy can be protected most effectively by technologies that avoid or at least minimize personal data that are exposed at network sites, and are thus providing anonymity, pseudonymity, unlinkability or unobservability. However, such technologies cannot be applied in applications where personal data have to be processed.

Other privacy technologies can technically control that personal data are only used according to legal provisions. P3P is a technology, which enforces that personal data is only forwarded with the user's informed consent. According to data protection legislation, informed user consent is often required for the legitimacy of data processing.

5.2 Platform for Privacy Preference Project (P3P)

Self-determination for end users is a key issue. People's views on privacy differ a lot between individuals, and our willingness to give away information in order to gain convenience must be respected.

One simple way to accomplish this would be to ask the end user before making a transaction. However, to increase usability, we need to find a way for the user to enter personal settings once and for all, without having to re-enter them for each connection.

P3P provides developers of user agents, such as web and WAP browsers, with a specific privacy policy format, that can be parsed and matched against the end user's preferences.

5.2.1 P3P Agreement

How a P3P agreement is done is fully described in [P3P]. The P3P user-agent will typically, when an HTTP request is made, fetch a reference file, which is a site map, matching policy file with pages or parts of the site, and is typically stored at a well-known location at a website, "/w3c/p3p.xml". According to this reference file, the appropriate policy file will be retrieved, and matched against the user's preferences. If the there is a match, the page will be requested, and if not, the user-agent will take some kind of action to warn the user.

During the agreement, little or no information needs to be submitted. Minimal data collection should take place, and data that is collected is used in only non-identifiable form. This is called the "safe-zone".

5.2.2 A P3P User Agent

There will be various kinds of P3P user agents:
Plug-ins, browser built-in or proxies
Those that only inform the user, and those that will take some kind of action
Those that perform agreement on the user's explicit demand, or always
In mobile devices, user agents will be built-in, apparently, but proxies that act as trusted third parties are also possible. When we say trusted, we mean that in order to be responsible for the tremendous amounts of personal data that such a proxy would hold, trust is absolutely necessary.

6. THE PiMI PROTOTYPE PROJECT

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

W3C suggests that CC/PP be used together with P3P to ensure the end user's right to self-determination. As discussed in section 4, this is particularly important in mobile Internet environments.

The PiMI Prototype project started as a joint venture between Ericsson and Karlstad University in March 2001. The PiMI project goal was to implement P3P user agents controlling the dissemination of CPI in mobile Internet environments by the means of Minimal Profile Conveyance (see section 6.1) as described in [Nilsson et al. 2001].

6.1 Minimal Profile Conveyance

CPI is represented by means of a profile, see section 3.4, which comprises a set of components. Each component is a placeholder for related attributes.

In [Nilsson et al. 2001], we suggest that the user define a minimal CPI profile, containing only information that she considers completely harmless, or where there is an understanding that this information may be necessary for some reason. This minimal profile can be used:

- For accessing non-P3P enabled web sites or web sites that do not meet the user's P3P privacy preferences
- For serving third party requests to the WAP Gateway for cached profiles (such as for WAP push content generation)
- For communication in the "safe-zone" before a P3P agreement (within the "safe-zone", however, no CPI is needed, so that a completely empty profile could be used instead)

The end user also has to define a full CPI profile to be used when there is a successful P3P agreement on a general basis, i.e. the site is P3P compati-

ble, and the general information in the site's P3P policy file suites the end user's privacy preferences. All CPI attributes in this full profile must be agreed upon, i.e. there must be a corresponding P3P policy statement that corresponds to the end user's preferences for these attributes. Otherwise the CPI attributes will not be transmitted.

Here is one example: A user may be able to give away image capability, i.e. the fact that she can view images, and screen size, i.e. the size of the screen in pixels, in order to get a better experience when viewing a page. However, to sites that will grant her access to the information that they store, she may be willing to give away also the browser name, i.e. the name of the user agent, so that everything about the browser and its capabilities can be fetched by the origin server, and the browser version, i.e. the exact version as well.

In this example, the image capability and screen size are examples of minimal profile content, while the browser name and version belong to the full profile. The access right is the general information that needs to be agreed upon. If there is no statement for a specific set of data, it will not be transmitted.

The WSP suspend and resume mechanisms can be used for retransmission of the data in the full profile that have been agreed upon.

6.2 Overview

The PiMI system consists of both a proxy-based and a browser built-in P3P user-agent. The browser built-in user agent solution guarantees that the user has direct control over her privacy preferences. However, the communication during the P3P agreement over WSP [WSP] is quite slow and costly. With the proxy-based solution, the user agent's communication during a P3P agreement is done from by a HTTP privacy proxy and thus takes place via wireline communication. However, as in this case the proxy has control over the user's privacy preferences, it should be either under direct control of a trusted third party (TTP) or of the user (e.g., running on the user's PC).

In the prototype project, we have so far only developed P3P preferences and policies for CPI information. An example P3P policy file for UAProf attributes, written within the project, can be found at [P3P & UAProf]. However, the concept can also be used for any other kind of personal data to be transmitted from the device, e.g. location data, name, credit card number etc.

In this prototype, we only test for CPI information. However, the same principle can be used for any other kind of data to be transmitted from the device, e.g. location data, name, credit card number etc.

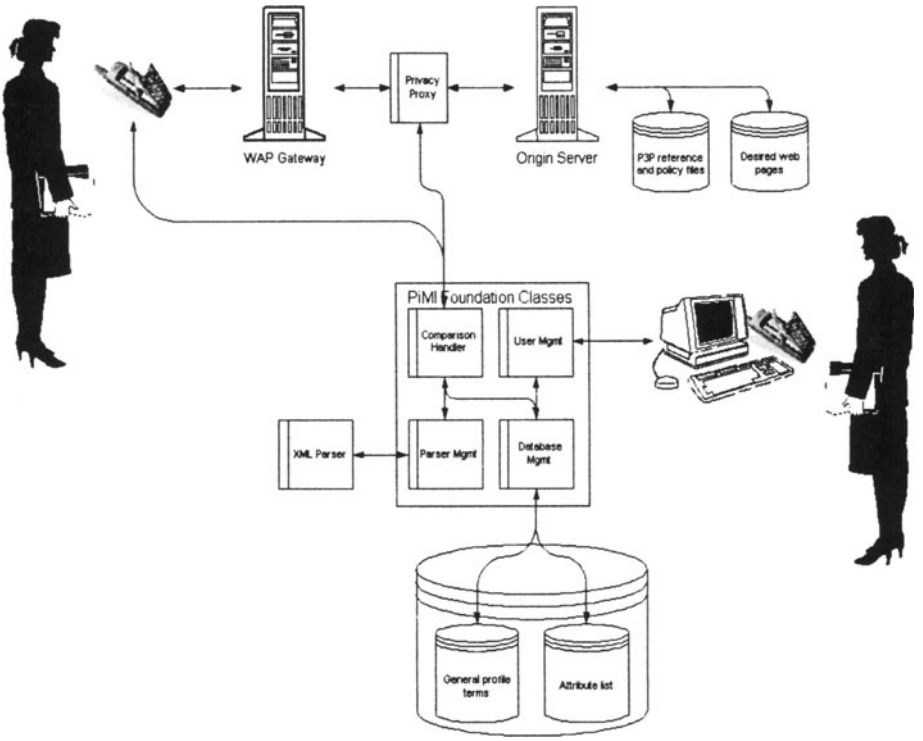

Figure 2. The PiMI Architecture

Both the browser built-in and proxy user-agents use the PiMI foundation classes that allow the end user to enter preferences from an HTML as well as a WML interface, and have them stored in flat files.

The comparison handler will retrieve the reference file according to the well-known location concept, find the policy file, for example the one described in [P3P & UAProf], and compare the general information (in this case access information). If there is a match, it will compare the data in the full profile, otherwise the data in the minimal profile. After this, it will either retrieve the web page, passing on the information agreed upon, or else warn the end user about the parts that failed, and ask whether she consents to providing the information anyway.

6.3 Results and Suggestions

The amount of attributes for which a P3P agreement has to be made widely exceeds the amount of attributes used in traditional web environments, as discussed in 4.

We realized that it is wise to use three categories for each CPI attribute:

- **Minimal** - this attribute is part of the minimal profile, and can be given away to any site
- **Full** - this attribute is part of the full profile, and can be given if the user's preferences for this attribute match the site's policy (i.e., the user gives her implicit consent)
- **Never** - this attribute will never be given away, without the end user's explicit consent, (i.e., the user is explicitly asked)

It is technically possible to have the end user define a range of profiles, and select among them before each transmission. However, there is a conflict between user friendliness and privacy friendliness. The principle tried in the PiMI project is one first step towards self-determination without disturbing the end user more than necessary.

7. CONCLUSION

In this paper, we have discussed why the user's privacy is at risk in the mobile Internet. To protect privacy, a holistic approach, including legal means, privacy-enhancing technologies as well as educational measures for raising awareness and teaching users how to apply privacy-enhancing technologies is needed.

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 only may 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.

The P3P protocol can be used to enforce user control over personal user data, such as CPI including location data, allowing the transfer of CPI and location data only if there is an informed consent of the user. Thus, the WAP P3P user agents developed in the PiMI prototype project can be used to protect location data according to the requirement of the EU directive proposal.

Acknowledgement

The HumanIT research program at Karlstad University has funded parts of this work. We therefore want to thank HumanIT for their support.

REFERENCES

[3GPP] "3G Partnership Project". http://www.3gpp.org/.

[CC/PP] World Wide Web Consortium. "Composite Capability/Preference Profiles (CC/PP): Structure and Vocabularies". W3C Working Draft. 15 March 2001. http://www.w3.org/TR/CCPP-struct-vocab/

[CC/PP Note 1999] F. Reynolds, J. Hjelm, S. Dawkins, S. Singhal. "CC/PP: A user side framework for content negotiation". W3C Note. July 1999. http://www.w3.org/TR/NOTE-CCPP/

[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] Commission of the European Communities COM(2000) 385. "Proposal for a Directive of the European Parliament and of the Council". July 2000. http://europa.eu.int/comm/information_society/policy/framework/pdf/com2000385_en.pdf

[EU Telecommunication Directive 1997] European Parliament. "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".

[Hjelm et al. 2000] J. Hjelm, M. Nilsson. "Position dependent services using metadata profile matching". iNet, the Internet Society Conference. July 2000. http://www.wireless-information.net/Johan/Engelska/inet00-paper-01.htm

[Holvast 1993] J. Holvast. "Vulnerability and Privacy: Are We on the Way to a Risk-Free Society?". J.Berleur et al. (Ed.): Facing the Challenge of Risk and Vulnerability in an Information Society, Proceedings of the IFIP-WG9.2 Conference, Elsevier Science Publishers B.V. (North-Holland), 1993. Namur May 20-22, 1993.

[ETSI GSM 03.71] ETSI Specification GSM 03.71 V7.3.0. ETSI Technical Specification GSM 03.71. February 2000.

[MeT Overview] "MeT Overview White Paper, Version 2.0". January 29, 2001. http://www.mobiletransaction.org/pdf/White%20Paper_2.0.pdf

[Nilsson et al. 2001] Mikael Nilsson, Helena Lindskog, Simone Fischer-Hübner. "Privacy Enhancement in the Mobile Internet". In Proceedings of Security and Control of IT in Society-II, IFIP SCITS-II. Bratislava, Slovakia, June 15-16, 2001. http://privacy.lindskog.ws/pimi.pdf

[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". 23rd September 1980.

[P3P & UAProf] H Lindskog. "A Sample P3P Policy for UAProf". May 2001. http://privacy.lindskog.ws/p3p_policy4uaprof.html

[P3P] World Wide Web Consortium. "The Platform for Privacy Preferences 1.0 (P3P1.0) Specification". W3C Working Draft. 28 September 2001. http://www.w3.org/TR/P3P/

[RFC 2068] R. Fielding et. al. "Hypertext Transfer Protocol -- HTTP/1.1". World Wide Web Consortium. January 1997. http://www.w3.org/Protocols/rfc2068/rfc2068

[Rosenberg 1992] R. Rosenberg. "The Social Impact of Computers". Academic Press. 1992.

[Schilit 1995] William Noah Schilit. "A System Architecture for Context-Aware Mobile Computing". 1995. http://www.fxpal.xerox.com/people/schilit/index.htm

[UAProf] WAP Forum. "User Agent Profile Specification". WAP Forum Working Draft. 2001. http://www.wapforum.org/

[WAP] WAP Forum. "Wireless Application Protocol, Wireless Application Protocol Specification". 2001. http://www.wapforum.org/

[WBXML] WAP Forum. "Wireless Application Protocol, WAP Binary XML". WAP-192-WBXML. 25-July-2000. http://www.wapforum.org/

[Westin 1967] Alan Westin. "Privacy and Freedom". New York, 1967.

[WSP] WAP Forum. "Wireless Application Protocol, Wireless Session Protocol Specification". WAP-203-WSP. 4-May-2000. http://www.wapforum.org/