Privacy Requirements for Mobile Services

Candidate Version 1.0.1 – 12 Dec 2006

Open Mobile Alliance

OMA-RD-Privacy-V1_0_1-20061212-C

Contents

Figures

Tables

1. Scope (Informative)

Privacy has three aspects: personal, territorial and informational. In an IT context, personal privacy is about content filtering and other mechanisms to ensure that end users are not exposed to whatever violates their moral senses, while territorial privacy is about protecting the user's property - e.g. the user equipment - from being invaded by undesired content, such as SMS or email messages. Informational privacy is about data protection, and the users right to determine how, when and to what extent information about her is communicated to other parties, and the execution of this right might be based on her knowledge about what the other party's intention is.

This document defines general privacy requirements within the OMA framework. In addition to general privacy requirements, some services or service enablers may have specific requirements, which are addressed in respective specifications.

The requirements contained in this document are limited to the protection of personal data (informational privacy).

Personal data is

- Information that is tied to a Data Subject such as
  - Address,
  - Telephone number,
  - Social security numbers
  - Network data that could uniquely locate a Data Subject
  - Any other personally identifiable information
- Information about a Data Subject such as bio data, calling habits, user preferences, disposition to be contacted, etc
- Information which when combined with other information could infer the identity of a Data Subject, e.g. IP address, User Agent profile, etc.
- Information which when stored could have specific requirements, e.g. cookies and location data

Even though the following are aspects of IT privacy, they are outside the scope of this work item:

- Protection from unsolicited communication (territorial privacy); see also the informative section 9
- Preventing access to undesirable information, e.g. protecting children (personal privacy)

This document contains a non-exhaustive list of requirements that are mandated by legislation, and those that are not necessarily covered by legislation but are nevertheless considered industry best practices. Both the market/social expectations and legislative mandates are captured by use cases.

2. References

2.1 Normative References

[EU95]
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
Official Journal L 281, 23/11/1995 P. 0031 – 0050
http://europa.eu.int/eur-lex/en/search/search_lif.html

[EU02]
Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
Official Journal L 201, 31/07/2002 P. 0037 – 0047
http://europa.eu.int/eur-lex/en/search/search_lif.html

[EU97]
Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector
Official Journal L 024, 30/01/1998 P. 0001 – 0008
http://europa.eu.int/eur-lex/en/search/search_lif.html

[FCC]
FCC THIRD REPORT AND ORDER AND THIRD FURTHER NOTICE OF PROPOSED RULEMAKING in the Matter of Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information.
http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-02-214A1.pdf

[HTTPSM]
HTTP State Management Specification, WAP-223-HTTPS-20001213-a, WAP Forum.
http://www.openmobilealliance.org/wapdocs/wap-223-httpsm-20001213-a.pdf

[OECD]
OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (23rd September, 1980)
http://www1.oecd.org/publications/e-book/9302011E.PDF

[PCP]
OMA Location Privacy Checking Protocol Requirements: OMA-PCPReq-V1_0_2-20030909-D

http://www.openmobilealliance.org

[PROXY]
OMA Requirements Specification: WAP Proxy-Based Redirect: OMA-RD_WAPproxyBasedRedirect-V1_0-20030520-C

http://www.openmobilealliance.org

[RFC2119]
"Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997,
URL:http://www.ietf.org/rfc/rfc2119.txt

2.2 Informative References

[OMADICT]
"Dictionary for OMA Specifications", Version x.y, Open Mobile Alliance™,
OMA-ORG-Dictionary-Vx_y, URL:http://www.openmobilealliance.org/

[FTC]
FTC PRIVACY ONLINE: Fair Information Practices in the Electron Marketplace, A Report to Congress Federal Trade Commission, MAY 2000.
http://www.ftc.gov/os/2000/05/index.htm#22

3. Terminology and Conventions

3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

3.2 Definitions

Anonymous Data Data rendered in such a way that the data subject is no longer *identifiable*. When determining whether a person is *identifiable*, account should be taken of *all reasonable means likely* to be used either by the controller or by any other person to identify the said person. [EU95]

Note: Examples of personal data that should be anonymised are web server log files

Attribute Provider An entity that provides attribute information. E.g. a Web Service that hosts Principal’s (i.e. Data Subject’s) attributes.

Consent Any freely given specific and informed* indication by which the data subject signifies his agreement to personal data relating to him being processed. [EU95]

** Consent provided by the data subject having obtained information about the purpose of the “processing” for which the personal data are intended*

Controller The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

Note: the Controller could for example be an operator, a service provider or, more generally, any entity that keeps or gathers personal data of the user.

Data Subject An identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. [EU95]

Note: within the context of this specification in general the Data Subject refers to a user of mobile services.

Personal Data Any information relating to an identified or identifiable natural person (“data subject”). [EU95]

Processing Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Processor A 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

Privacy Preferences Privacy Preferences express preferences for *Privacy Settings* of the data subject. Privacy Preferences may be expressed by the data subject or a third party, (e.g. by the employer for his employees) to the controller of Personal data. This expression can be manifested e.g using Privacy Controls in an application or web service, or expressed in a written or verbal form as long as it is recorded in a permanent manner for later verification and access.

Privacy Settings Information relating to Personal data of a data subject. Privacy Settings describe the rights and limitations of access to and processing of Personal Data Privacy settings may be expressed in terms of access rules that determine a policy with respect to the privacy protection of personal data of a user towards Requestors.

Note: In general, Privacy Settings for an application or service would implement particular values for parameters, offered by this application or service, which are used for privacy control.

Privacy Controls Privacy Controls of an application or service are the means (e.g. control buttons, preferences menu…), by which the application or service allows the user to set his Privacy Preferences

Recipient A 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom personal data are disclosed.

Note: the recipient could for example be a service provider, a user or an application on behalf of a service provider or user

Spy ware Software agents, programs or files deployed onto devices and programmed to look for Personal Data on a Data Subject (e.g. passwords, social security numbers, addresses, telephone numbers, credit card numbers, etc.) and to report it back to the originator.

Traffic Data May, inter alia, consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection, [EU02]

Traffic data is only relevant to the scope of privacy protection when when it is combined with other data which could then be used to identify an individual

3.3 Abbreviations

OMA	Open Mobile Alliance

4. Introduction (Informative)

Most if not all services in OMA architecture will require protection of personal data. Each service capability may have its own privacy requirements and will solve them in their own way. For instance location services can trigger on users entering an area, and perform actions, like sending a message to another individual according to stored user preferences. A game service may have other privacy requirements, such as remaining anonymous in a game. However, many of the requirements are common across these capabilities, resulting in the same problem being solved many ways.

Therefore, this specification aims to collect common requirements, and thus helps to create common solutions for OMA services. Each entity dealing with Personal Data must know to what other parties the information may be forwarded, or where to find out what rules are applicable.

This specification also investigates the impact of policy enforcement on the OMA architecture. Privacy policies should state the intent of usage from the content provider, with regards to purpose, recipient, and retention period, but also give information about how to address the processor of the data, and what to do when there is a dispute. The legal implications of privacy policies vary between countries.

It is important that the requirements that this document places on other groups match the requirements posed by legislation, but also that the user's right to self-determination is protected as much as possible. Focus must be on legal, user and business perspectives.

However, it is also important to bear in mind that the most essential aspects of user privacy appear when the user has already given up the user data, be it a simple IP number or much more sensitive data. Processing and storage of personal data, as well as sharing information with other parties, occur after data has been given up. OMA has no possibility to supervision and sanctions towards parties that do not adhere to legislative or other privacy-related aspects once the data has been shared.

Although seen primarily from the subscriber's and service providers' points of view, this document contains information applicable to network operators, terminal manufacturers, network system manufacturers, content and service providers.

In order to provide a proper market driven study of the requirements, the use cases contained in this document have been derived from service scenarios that are thought to be representative of the entire value chain for providing personalised services in mobile networks. In particular, the use cases will consider the normative requirements for meeting the regional regulatory directives where they exist

4.1 Roles in the Privacy Framework

The following figure gives an overview on the roles defined in the present requirements document:

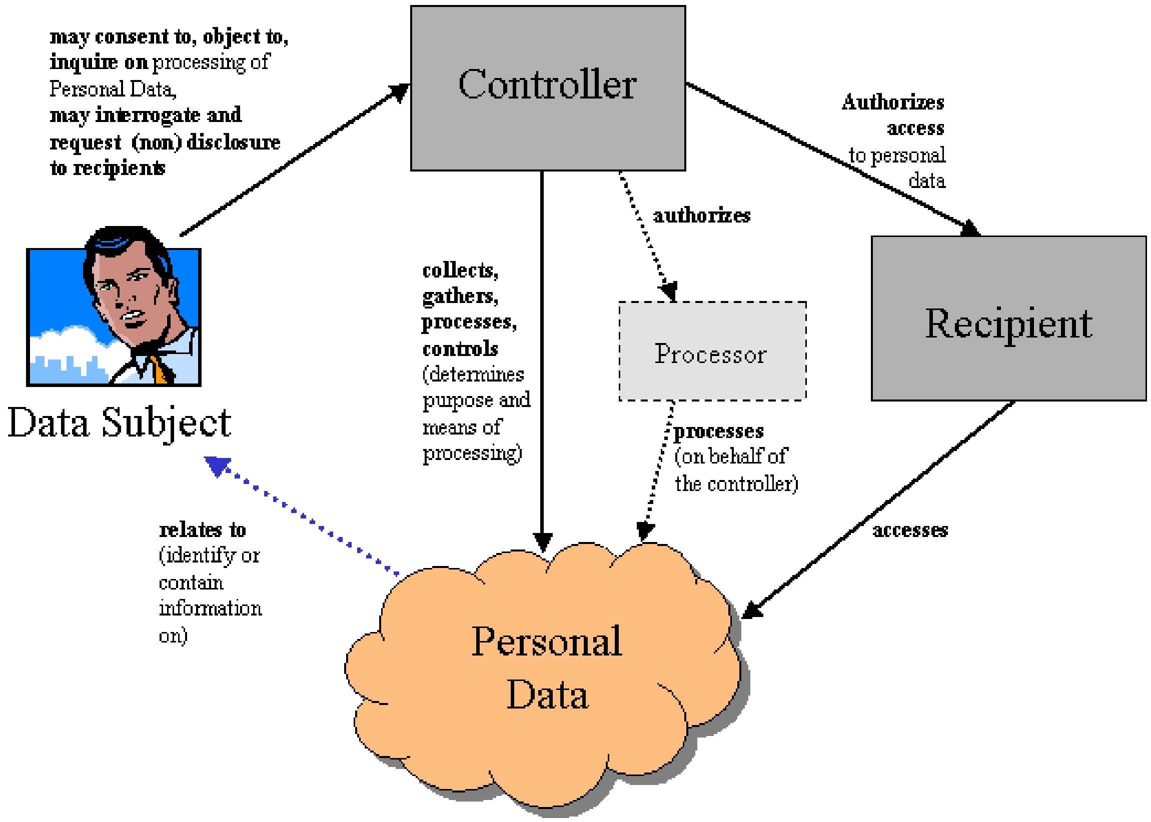
may consent to, object to, inquire on processing of Personal Data, may interrogate and request (non) disclosure to recipients
Controller
Authorizes access to personal data
authorizes
Data Subject
collects, gathers, processes, controls (determines purpose and means of processing)
Processor
Recipient
processes (on behalf of the controller)
relates to (identify or contain information on)
accesses
Personal Data

Figure 1: Privacy Roles

Figure 1 shows the roles and relationships between these roles that are considered in the present document.

- The **Data Subject** is the person being represented by some Personal Data. In general, within the context of this specification, the Data Subject refers to a user of mobile services.
  The present document is all about the privacy requirement a Data Subject has for his Personal Data with respect to the parties involved in controlling or having access to these data (i.e. the Controller, Processor and Recipient). The relationship between a Data Subject and the Controller expresses these privacy requirements.
  For example an operator - the Controller - may ask the user - the Data Subject - to give his consent to the disclosure of the user's mail address - i.e. some Personal Data - to a service provider - i.e. the Recipient.

- **Personal Data** relate to a particular data subject.
  Through Personal Data the identity of a Data Subject may potentially be derived (e.g. a telephone number would identify the user) and/or they contain other information on the data subject (e.g. preferred web-sites of the user).

- The **Controller** of Personal Data is the entity that is "in charge" of a Data Subject's Personal Data. The Controller could for example be an operator, a service provider or, more generally, any entity that keeps or gathers personal data of the Data Subject. The Controller determines the purposes and means of the processing of personal data.

- The **Processor** may have some of the duties of the Controller (concerning Personal Data) relayed to it and therefore be authorised to process (e.g. collect, record, store, make available…) a Data Subject's Personal Data on behalf of the Controller.
- A **Recipient** is an entity (e.g. a person, public authority, agency…) to whom Personal Data of a Data Subject may be disclosed by the Controller. A Recipient would request the Controller to access Personal Data. Depending on privacy settings of the Personal Data the Controller may pass these Personal Data to the Recipient.

5. Use Cases (Informative)

5.1 Use Case A: Controller Scenario

This use case presents a real-world example where the controller of the privacy parameters of a particular mobile device can interact with a privacy control function in different operator's networks in a consistent manner. This use case underscores the necessity to provide such a requirement in order to allow controllers with maximum flexibility in determining how and when the networks must enforce privacy rules when presented with requests for information from external applications.

5.1.1 Short Description

A multinational company provides wireless devices and provisions wireless services for its employees in different countries, using multiple network operators. The company desires to have a single IT application interact with the different networks in order to control privacy aspects of their employee's wireless equipment and services. It would also like to allow the employees to also have control over their preferences through the device itself, with appropriate IT controls.

5.1.2 Actors

Network operator A

Network operator B operates his network under a different administration (e.g. in a different country) that has differences in regional policy to A

A multinational company who has subscriptions with Network operators A and B. The company's IT department is the controller of privacy preferences of its employee's mobile devices.

Employees of the company who use the mobile devices. An employee may be a user of network operator A (i.e. have a network identity and services provided by operator A); he may be a user of network operator B or of both.

5.1.2.1 Actor Specific Issues

Network Operator A & B

Enforce privacy rules according to local jurisdictions which is characterised as carrying out the data subject's instructions as determined in their privacy preferences and policies. Thus, the network operator is providing the means for the data subject to determine how their information is used and made available to third parties.

Multinational Company (subscriber)

Wants to provision services to its employees

Wants of ease of control over privacy

Company employees (end-users)

Do not want their privacy violated by unauthorised applications

5.1.2.1 Actor Specific Benefits

Network Operator A & B

Provides secure services to its corporate clients

Multinational Company (subscriber)

Maintains productivity of its employees

Has a single application to interact with different networks serving its employees

Ensures that the privacy of its employees is not violated

Company employees (end-users)

Flexible means to consent to changes to privacy preferences

5.1.3 Pre-conditions

The company has implemented an application that controls the privacy preferences for all the users of mobile devices that it supplies. These privacy preferences could, for example, apply to location-based services or push services for that employee.

5.1.4 Post-conditions

A successful instantiation of the application results in the privacy preferences of a user of a mobile device in a wireless operator's network such that external applications may not obtain private information about the mobile (user) without querying the database.

5.1.5 Normal Flow

- The IT department of the company invokes an application to provide privacy settings for a mobile employee's PDA using services in operator A. This data includes authorization for external applications to push data to the PDA based on location and time of day
- The application interacts with a control function of Network Operator A in order to control access to the PDA when the operator receives push content from an external source.
- Subsequent pushes are only permitted, if they comply to the privacy settings set by the company. The enforcement of these privacy settings is done by Operator A.
- The IT department repeats the procedure for another employee, except that the application interacts with Network Operator B

5.1.6 Alternative Flow

- As above, except that the mobile user can access the database control function directly from his/her PDA.

5.2 Use Case B: New Service Authorisation

This use case demonstrates privacy management functionality where a user of location services is able to temporarily change his privacy preference preferences.

5.2.1 Short Description

In this use case example, the data subject is a user of location services. The user accesses a Map Service application that has not been previously configured by the user as a trusted service.

5.2.2 Actors

- Mobile End User
- Map Content Provider
- Location Service Provider
- Network Provider

5.2.2.1 Actor Specific Issues

User

- Wants to protect his privacy
- Wants flexibility form the services he uses

Map Content provider

- Make content available to privacy conscious (mobile) Users

Location Service provider

- Wants to authenticate 3rd party content providers
- Wants to protect its users' privacy

Network provider

- Wants to protect the User's privacy.
- Wants to authenticate Location Service provider
- Wants to authenticate the Map Content provider.
- Wants to authenticate the User.
- Wants to obtain consent of the User.
- Wants to check if passing on location information is legitimate and reject fraudulent requests.

5.2.2.2 Actor Specific Benefits

User

- Can access new services that can be trusted not to violate his privacy

Map Content provider

- Increases its customer (target user) base

Location Service provider

- Seen as a flexible, ("always ready") service provider

Takes share of revenue

Network provider

- Creating trust towards User.
- Seen as reliable business partner to Location Service and Map Content provider.

5.2.3 Pre-conditions

- Mobile handset with web browser sets up secure session with web application
- Mobile End User has subscribed for a location service and has accepted an agreement between himself and the Location Service Provider to allow new location based services to be introduced to him by first asking for his confirmation
- Location information can be displayed by mobile device

- Security infrastructure of network provider successfully authenticates the user

5.2.4 Post-conditions

Map service sends a map of the User's location.

5.2.5 Normal Flow

The user wants to download a map of his current location. He browses the web and finds a map service, which has not been configured as a trusted service in by his service provider. However, he has consented to a rule that allows new location-based services to be introduced to him by first asking for his confirmation for location usage. As the target, the user has set a limitation that only those new services, which agree to use the location data for providing a service to the target himself is using, may be introduced.

The following sequence describes the normal flow of events:

1. The user initiates a browsing session to a Map Content Provider. Map Content Provider notices that user is a mobile subscriber and asks him if he would like a map of his current location. The user answers "yes" and sends his mobile identity.
2. Using the target's identity, the Map Content Provider asks location from the Location Service Provider. The Location Service Provider authenticates the Map Service Provider. Then it checks if the Map Service Provider is on the list of trusted services, but the Map Service Provider is not found there.
3. The user receives notification of a location request and authorises the request.
4. The Location Service Provider passes the location request on to the Network Provider.
5. The Network Provider authenticates the User's consent and the Location Service Provider.
6. The Network Provider checks if the request is legitimate.
7. If the location request is legitimate sends the Network Provider a positioning response to the Location Service Provider.
8. The Location Service Provider passes the location response message to Map Service Provider.
9. Map Service Provider sends map of the User's current location to User.

5.2.6 Alternative Flow

An alternative to the normal flow would allow the user to remain anonymous towards the Map Content Provider:

1. The user initiates a browsing session to a Map Content Provider.
    a. The browsing session does not reveal the user's mobile identity to the Map Content Provider. The Map Content Provider asks the user if he would like a map of his current location and if so he would need to identify himself.
    b. The user decides not to give away his mobile identity to the Map Content Provider but to provide an alias, which can be verified by the Location Service Provider. By doing so - and possibly changing the alias for subsequent transactions - the user is able to assure that his true identity cannot be misused by the Map Content Provider in the future.
    c. Together with the user's answer "Yes" the alias is transmitted to the Map Content Provider.

2. Instead of using the target's identity the Map Content Provider uses the target's alias to ask for location from the Location Provider. The Location Provider resolves the user's alias to his mobile identity for determining the location, and subsequently reuses the alias when sending the location to the Map Content Provider.

The rest of the flow is the same as in 3.5.

5.3 Use Case C: Changes to Settings

This scenario illustrates the necessity for providing users whose personal data is subject to privacy protection (i.e. data subjects) with the flexibility to modify and expand their privacy preferences and not be restricted to doing so when they upgrade their device.

5.3.1 Short Description

Teresa is a young professional mobile subscriber who opts to upgrade her old voice + data based wireless handset to a new PDA style wireless device with built in camera. Teresa wants to keep her old mobile phone number but wishes to expand her privacy options in her user profile in order to make use of the host of new third generation mobile services available on her existing network.

5.3.2 Actors

- Mobile End User
- Network Provider

5.3.2.1 Actor Issues

User

Wants to access new mobile services

Wants to protect her privacy

Wants to keep her existing mobile number

Network Provider

Wants to retain valued customers by attracting her towards new multimedia services

Wants to be seen as a trusted operator

5.3.2.2 Actor Benefits

User

Confirmation of changes to privacy reassures user that her personal data remains protected

Can access new services without worrying about privacy

Feels like a valued customer

Network Provider

Generate revenue from new services

Retains customers

5.3.3 Pre-conditions

- User already has a subscription with her network operator

- User is deemed a highly valued subscriber by her operator and is offered a deal to upgrade her device

5.3.4 Post-conditions

Teresa successfully upgrades her device keeping her old telephone number but enhances the privacy preferences to reflect the more feature rich value added 3G services available through her subscription to her existing network operator

5.3.5 Normal Flow

Teresa decides to take up an offer from her network operator to upgrade her old 2.5G handset for a new 3G PDA device. She visits the High Street outlet of her network operator where the vendor is able to make the appropriate changes to her contract and to issue her with a new SIM and device but keeps her old mobile telephone number.

The initial upgrade transaction allows Teresa to leave with her new PDA enabled for voice calls only, but with instructions on how to initiate subscriptions to other services and change her user preferences.

Teresa invokes an application via a secure connection to her operator's web site and interrogates the settings of her privacy preferences via her user profile. She consents to changes to her existing settings pertaining to the use of her personal information and makes choices on new options enabled by her upgraded subscription.

The application responds to her choices by reminding her to make careful informed choices when changing privacy preferences and asks her to confirm the changes.

5.3.6 Alternative Flow

Alternatively, the user can access her rules database application via her PDA as and when she is notified of new services when they become available, (e.g. by Push notification).

5.4 Use Case D: Management of Privacy Settings

This use case illustrates the requirement for allowing end users to add new services and allow them to inherit their privacy preferences in an easy fashion.

5.4.1 Short Description

Mary is a busy 23-year-old junior executive working for a large multi-national company. She also has many other interests outside work and has a healthy personal life and many friends. She needs to keep in touch with her friends and work contacts during the day.

Mary has over 100 contacts in 3 “buddy lists”. Each list comes with separate privacy settings.

She is known for her “appetite” for new mobile services, especially those that enable her to manage her work and personal life through her new mobile device, and often likes to try out new mobile services.

5.4.2 Actors

- End User
- Content Provider
- Service Provider
- Network Operator

5.4.2.1 Actor Specific Issues

End User

Wants to stay in touch, but not worry about her privacy

Wants to easily manage her contacts lists

Wants value from her device

Cost of service not so much an issue, staying in touch is more important

Try before Buy

Content ProviderWants to create content that is interoperable across service providers and devices

Wants to protect his content

Wants to generate revenue from content

Service Provider

Wants dependable, "always-on" value added services

Wants to advertise other services

Wants to take a share of the revenue

Authenticate content providers

Authenticate users

Network Operator

Provide reliable delivery mechanism for content provided

Provide capability for storing privacy settings

Be able to take a share of the revenue

5.4.2.2 Actor Specific Benefits

End User

Can add new services and allow them to inherit her existing privacy preference preferences

Can access her user preferences via a single application via her mobile device or PCContent Provider

Faster take-up of interoperable content

Service Provider

Is seen as a trusted provider of services

Get revenue from service usage

Network Operator

Get revenue from service usage

Securely controls privacy settings of users

5.4.3 Pre-conditions

- Mary has a subscription with her service provider

- Mary has a Presence and Instant Messaging capable terminal with picture messaging
- Service Provider has a billing agreement with operator
- Chat Content Provider has an agreement with Service Provider5.4.4 Post-conditions
- Mary successfully adds the new presence enhanced chat service to her device
- The new service interoperates with the existing properties for Mary's contact lists
- She also successfully adds new names to her contact lists and gives them access according to the properties associated with each contact list

5.4.5 Normal Flow

- Mary receives an advertisement "pushed" to her mobile device about a new presence enhanced "chat" service with easy to use icons and which allows her to make use of the picture messaging capability of her mobile device.
- Mary browses the web site of her Service Provider to find out that the service is compatible with her device
- Mary likes the demo and downloads the service to her mobile device
- The Service Provider requests Mary to fill in a simple questionnaire about her current contacts and whether she would like them to be added to this new service
- Mary wants this new chat service to use her existing privacy preferences rather than create new ones
- Mary adds new names to her existing lists: friends", "family" and "work" by making use of an easy to use interface with pop-up windows and sliders to set properties according to type of contact list

5.4.6 Alternative Flow

None

5.5 Use Case E: User Prefers to Enable Proxy-Based Redirect

This use case is taken from the OMA Proxy based re-direct Requirements Document, [PROXY] to illustrate the privacy requirements related to WAP proxies.

5.5.1 Short Description

Proxy-based redirect may not be considered desirable by all users or for all requests, for example due to concerns over privacy or security. Proxy-based redirect may also be incompatible with certain WAP device features, e.g. domain-based proxy selection. To address these concerns, WAP devices may control the use of proxy-based redirect by announcing a preference to enable or disable proxy-based redirect for the current WAP session, or for the current request. In addition, WAP proxies may provide users with a similar proxy-based preference applicable to all requests (e.g. as a user profile attribute). Support for device-based control is mandatory. Support for a proxy-based preference is optional. The WAP proxy may assume a default value for proxy-based user preferences.

WAP device controls of proxy-based redirect may be invoked as a related function of more general user preferences, e.g. as optimisation, privacy, or security related controls. If so, the use of proxy-based redirect must be consistent with the current setting for the related controls.

5.5.2 Actors

End-user

WAP proxy operator

Web-based service provider

5.5.3 Pre-conditions

The user's device and the WAP proxy both support proxy-based redirect.

A user preference to enable proxy-based redirect is expressed either through configuration of the device or WAP proxy, or assumed by default.

The web-based service utilizes redirection for the URL in the user device request.

5.5.4 Post-conditions

Content at redirect URLs is retrieved by the WAP proxy on behalf of the user, if appropriate for the specific request.

5.5.5 Normal Flow

1) The user selects a link in a web page being viewed. A web request is sent to the origin server.

2) The WAP proxy forwards the request to the origin server.

3) The origin server replies with a redirect to another URL.

4) The WAP proxy receives the redirect response. The WAP proxy determines that the device has indicated a user preference to enable proxy-based redirect, and that proxy-based redirect is appropriate for the current request. The WAP proxy sends a web request for the content at the URL indicated in the redirect response.

5) The origin server replies with the content for the URL.

6) The WAP proxy forwards the reply to the user, with an indication of the base URL for the content.

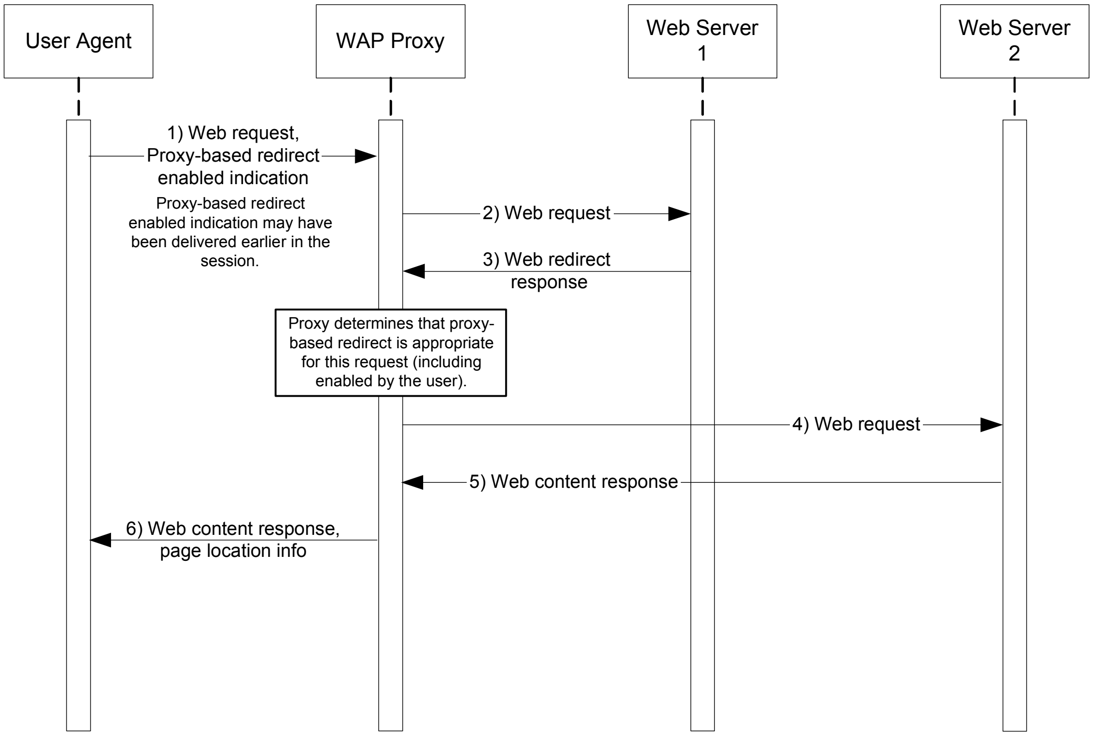
User Agent
WAP Proxy
Web Server 1
Web Server 2
1) Web request, Proxy-based redirect enabled indication
Proxy-based redirect enabled indication may have been delivered earlier in the session.
2) Web request
3) Web redirect response
Proxy determines that proxy-based redirect is appropriate for this request (including enabled by the user).
4) Web request
5) Web content response
6) Web content response, page location info

Figure 2: Use Case E: Normal Flow

5.6 Other Use Cases Motivating Requirements

5.6.1 Use Case F: Granularity of Data Collection

It may be necessary to track the location of a user or device for billing purposes. This means that the information collected should never be more granular than is strictly needed to render the relevant bill where possible. For example, if billing is based on the city of origin then it should not be necessary to track the street or building location of the user.

5.6.2 Use Case G: Device Sharing

A user may want to use a single mobile device and apply a business, social, or other persona to it when accessing the network. Accordingly, they may wish to apply a different set of privacy preferences to each persona. Controllers may want to improve performance or simplify workflow by caching privacy preferences based on a device ID. This could inadvertently cause the release of sensitive information.

5.6.3 Use Case H: Trustworthiness of Personal Data and Privacy Preferences

- A user may update her privacy preferences and access lists on their device. The changes may not get propagated to the network immediately. However, controllers are obliged to update changes as soon as possible and without delay. Where changes cannot be made immediately and there may be a delay, a request may be made to access the user's information and the network either uses cached information on the preferences or makes assumptions about access where applicable preferences exist in lieu of getting an accurate response from the device. The user is informed when they first set their privacy preferences that it may take time for changes to be implemented to their settings.

- The user is given a choice to allow the release of cached information to a requesting party. So, when requests for types of personal data that may change over time, are made, the user may want to indicate in her preferences that either no information is available or that cached information is available.

5.6.4 Use Case I: Rights of the Owner of the Device

- A company purchases devices for use by its employees. The company, as the owner, may want to control the device's settings in order to avoid, for instance, the loss of intellectual or physical property. E.g. the company is able to control the device user's permissions to download certain files from the company's Intranet.

- A parent purchases a device for use by its child. The parent, as the owner, may want to control the device's settings in order, for instance, to increase the child's protection.

- However, in respect of data processed by the network, the *user's* rights need to be respected by the Network Provider. For example, regardless of the subscriber's (e.g. a company or a parent) requests:

  - The Users' communications is not interfered with or intercepted without lawful authority or the user's consent, for example:

    - Cookies or spy ware are not placed on the user's device by the Network Provider without the user being informed of his right to refuse except, for instance where the sole purpose is to facilitate technical transmission or where it is strictly necessary to provide an online service explicitly requested by the user;

    - The Users' rights to bar identity presentation on a per call basis is not overridden without lawful authority interception or the user's consent;

    - The Users' right to consent to being located is not overridden without lawful authority interception or the user's consent;

  - The User's rights to temporarily block processing of location data (using a simple means which is free of charge) on a per connection or transmission basis is not be overridden without lawful authority interception or the user's consent,

5.6.5 Use Case J: Anonymous Attribute Sharing

This scenario illustrates how user's attribute information can be transferred anonymously to a service. Attributes are considered to be a particular type of personal data.

5.6.5.1 Short description

Consider the case where a user has an account with an Operator (acting as an Identity Provider). The user stores the zip code of his residential address and his language preference at a certain Attribute Provider 1 (AP1). The zip code of the user's current location may be obtained from a Location Attribute Provider (AP). The user has set the appropriate permissions for the release of his attributes stored at AP1 and Location AP.

The user uses his mobile terminal to access a service provider, CustomizedWeather.com, which provides weather information. The service provider, CustomizedWeather.com, requires the user's current and permanent zip code, as well as the user's language preference in order to provide the user with a customized weather report. Note that CustomizedWeather.com does not care about the identity of the user. This means that if the same mobile user revisited CustomizedWeather.com, there is no way for CustomizedWeather.com to identify that it is the same user browsing its site.

When the mobile user browses CustomizedWeather.com, it contacts the Operator in order to obtain the address of the attribute provider that stores the user's current and permanent zip code, as well as the user's language preference. Since the Operator has authenticated the mobile user, the Operator knows the identity of the user, and hence is able to determine the suitable attribute providers that store this information (since the Operator acting as IdP also provides discovery service). The Operator indicates to CustomizedWeather.com that the user's permanent zip code and language preference can be obtained from AP1, while the user's current zip code can be obtained from Location AP. CustomizedWeather.com then requests the user's permanent zip code and language preference from AP1, and requests the user's current zip code from Location AP. AP1 and Location AP check the permissions associated with these attributes, and release the attributes to CustomizedWeather.com. Note that throughout this entire flow, CustomizedWeather.com has no idea about the identity of the user. One may also note that CustomizedWeather.com does not require the user to have an account with it. Since such anonymous attributes are seamlessly transferred from an attribute provider (AP1 or Location AP) to the service provider (CustomizedWeather.com), the mobile user does not need to manually enter this information using his input-constrained numeric keypad. This then enhances the overall mobile user experience.

Since such anonymous attributes are seamlessly transferred from an attribute provider (AP1 or Location AP) to the service provider (CustomizedWeather.com), the mobile user does not need to manually enter this information using his input-constrained numeric keypad. This then enhances the overall mobile user experience.

5.6.5.2 Actors

- User – end user using a mobile device
- Operator – Mobile operator acting as an Identity Provider (IdP) and offering single sign on service and discovery service
- CustomizedWeather.com – Service provider providing customized weather information.
- Attribute Provider 1 – an entity providing user's permanent zip code and language preference information
- Location AP – an entity providing the user's current zip code

5.6.5.3 Pre-conditions

- User has an account with an Operator (acting as an identity provider and providing discovery service)

Operator has authenticated the user.

User has stored his permanent zip code and language preference at Attribute Provider 1 (AP1).

User's current zip code information is obtained from Location AP.

User has federated/linked his account at AP1 (and Location AP) with that at the Operator so that the Operator may provide discovery service for the user's attributes stored at AP1 (and Location AP).

User has agreed with operator, that neither his phone number nor any other identifying information will be given out of operator domain but has given operator permission to share his attributes with selected services.

User does not necessarily have an account with CustomizedWeather.com.

5.6.5.4 Post-conditions

- The user's permanent zip code and language preference information have been obtained by CustomizedWeather.com from AP1.
- The user's current zip code has been obtained by CustomizedWeather.com from the Location AP.
- CustomizedWeather.com provides a customized view of the user's weather – both at the user's current location as well as at the user's permanent location – using the user's preferred language.

5.6.5.5 Normal Flow

1. User accesses CustomizedWeather.com service using the browser on his terminal
2. CustomizedWeather.com requires the user's current and permanent zip code as well as the user's language preference in order to provide the user a customized weather report.
3. CustomizedWeather.com contacts the Operator to determine the attribute providers that store the user's current and permanent zip code and the user's language preference.
4. Since the Operator has already authenticated the user, the Operator knows the identity of the user, and the location of the attribute providers that store the user's attributes.
5. Operator and CustomizedWeather.com agree on the identifier of the user to be used for attribute exchange. Identifier does not reveal the identity of the user.
6. Operator responds to CustomizedWeather.com that AP1 provides the permanent zip code and language preference information of the user, while Location AP provides the current zip code of the user.
7. CustomizedWeather.com requests permanent zip code and language preference information from AP1, and current zip code information from Location AP.
8. After ensuring that the user permissions allow the release of such information, AP1 releases the permanent zip code and language preference information to CustomizedWeather.com, and Location AP releases the current zip code information to CustomizedWeather.com.
9. CustomizedWeather.com provides a customized view based on the zip code and language preference of the user.

5.5.6 Alternative Flow

1) The user selects a link in a web page being viewed. A web request is sent to the origin server.

2) The WAP proxy forwards the request to the origin server.

3) The origin server replies with a redirect to another URL.

4) The WAP proxy receives the redirect response. WAP proxy configuration indicates that proxy-based redirect is enabled for the user. The WAP proxy determines that proxy-based redirect is appropriate for the current request. The WAP proxy sends a web request for the content at the URL indicated in the redirect response.

5) The origin server replies with the content for the URL.

6) The WAP proxy forwards the reply to the user, with an indication of the base URL for the content.

6. Requirements (Normative)

Requirements for privacy arise from three sources: regulation, market expectations and social issues. For the regulatory source, the Directives of the European Union are used to cover legal requirements in general. Other requirements are derived from market needs and end user experiences.

6.1 Market Requirements

Label	Description
MRKT-1	Developing trust between individuals and businesses depends on installing confidence that Personal Data is securely protected and not misused, even if that individuals needs are not necessarily covered by regulation. From a market perspective, individuals want to use products and services, which take good, care of their information, and providers of the products and services want to meet the expectations of their customers. In particular, OMA service enablers SHOULD: • Be provided with a common set of functions for establishing and enforcing privacy policy in a consistent way • Reduce the cost of service deployment by o Re-use existing privacy practices o Achieve interoperability with existing service platforms • Encourage the uptake of new and existing mobile services by o Promoting trust between subscribers and service providers o Safeguarding personal or proprietary information o Addressing the need to protect the user's device against spam (messages, content, downloads) from third parties, see section 9.

Table 1: Market Requirements

6.2 High level requirements

The following is a list common technical requirements on service enablers that may process personal data on individual data subjects.

Note: In the following, the requirement either refers to a normative article from legislation or a use case. The letter preceding the number and placed after the requirement refers to the use case identified in section 5.

6.2.1 Requirements on Controllers/Processors of Personal Data

Label	Description
CONTPROC-1	Service enablers MUST provide a mechanism to allow controllers/processors to provide the following information on privacy settings to data subjects: - o The identity of the controller and processor, if any o The purposes of the processing for which the data are intended o The categories of data concerned o The recipients or categories of recipients of the data o The existence of the right of access to and the right to rectify the data
CONTPROC-2	In addition, service enablers MUST provide a mechanism to allow controllers/processors to inform data subjects, at the time of collecting personal data from the data subject, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply. **[EU95] Article 10, 11**
CONTPROC-3	The controller of the privacy preferences SHOULD guide data subjects about making careful choices concerning their privacy preferences **C2**
CONTPROC-4	Service enablers SHALL provide a means to obtain the informed consent at the time of collecting personal data from the data subject. **B2**
CONTPROC-5	Enforcement of any changes to privacy settings by the controller/processor after a data subject or a third party has expressed new or modified privacy preferences SHALL apply immediately upon update completion. **C3**
CONTPROC-6	It SHALL be possible for to the controller/processor of a data subject's personal data to designate third parties to express privacy preferences**. A1**
CONTPROC-7	An application of a third party SHALL be able to interact with multiple control functions of several controllers/processors in order to express privacy preferences. **A2**
CONTPROC-8	A controller's/processor's control function SHALL be able to interact with multiple third parties. **A3**
CONTPROC-9	The network operator SHOULD be able to interwork with several company's IT departments, each with different privacy requirements. **See informative section 9 A4**
CONTPROC-10	Service enablers MUST provide a mechanism to allow controllers/processors to assess and ensure the degree of accuracy of personal data before processing. **H1**
CONTPROC-11	Where a data subject updates her privacy preferences, controllers SHOULD update the changes to the privacy settings as soon as possible. **H2**
CONTPROC-12	Data subject's SHOULD be informed when they first set their privacy preferences that it may take time for changes to be implemented to their privacy settings. **H3**
CONTPROC-13	The data subject SHOULD be given an option to allow either the release of cached personal data or to indicate that no personal data is available, (note, this clause is applicable to personal data that is sensitive to time like location data). **H4**
CONTPROC-14	Before any data can be collected by an application, **B2**

CONTPROC-14a	○ The informed consent of the data subject MUST be obtained
CONTPROC-14b	○ The controller SHALL process only data that is necessary for the purposes of performing a contract to which the data subject is party or otherwise be permitted by law.
CONTPROC-15	In cases, where the data subject's control over his/her privacy preferences is, in whole or in part restricted by a controller or a processor, the controller/processor SHALL be able to inform the data subject of his/her limitations with regards to controlling the privacy preferences. Furthermore the data subject MUST be informed of his/her exposure with regards to the privacy preferences that may be set by the controller/processor. **I1** Note: This requirement specifically relates to corporate privacy requirements from North America i.e. where a company (= controller) owns a mobile device, which is used by an employee (= data subject)
CONTPROC-16	However with respect to data processed by the network, *user* rights MUST also be respected by the Network Provider. In particular, regardless of the subscriber’s requests or privacy settings **I2**:
CONTPROC-16a	○ Data subject’s communications MUST not be interfered with or intercepted without lawful authority or the data subject’s consent
CONTPROC-16b	○ Cookies or spy ware MUST not be placed on the data subject’s device by the Network Provider without the data subject’s being informed of his right to refuse except where the sole purpose is to facilitate technical transmission or where it is strictly necessary to provide an online service explicitly requested by the data subject;
CONTPROC-16c	○ The data subject’s rights to bar identity presentation on a per call basis MUST NOT be overridden without lawful authority interception or the data subject’s consent;
CONTPROC-16d	○ The data subject’s right to consent to being located MUST NOT be overridden without lawful authority interception or the data subject’s consent;
CONTPROC-16e	○ The data subject’s rights to temporarily block processing of location data (using a simple means which is free of charge) on a per connection or transmission basis MUST NOT be overridden without lawful authority interception or the data subject’s consent;
CONTPROC-17	If different personal data of the same data subject can be stored on different entities, then: -
CONTPROC-17a	• The entity storing the personal data SHALL be able to indicate its policy for personal data release to the data subject. **J1**
CONTPROC-17b	• There SHALL be guidelines for an entity to check permissions prior to release of personal data **J2**
CONTPROC-17c	• Service Provider’s SHOULD be able to query for a data subject’s personal data without associating the identifier used in the query with the identity of the data subject. **J3**
CONTPROC-17d	• Service Provider’s SHOULD be able to associate usage directives with the corresponding personal data that are being requested. **J4**
CONTPROC-17e	• The data subject SHALL be able to set permissions for the release of data subject’s attributes stored at an entity. **J5**

Table 2: High Level Requirements on Controllers/Procesors of Personal Data

6.2.2 Requirements coming from Data Subjects

Label	Description
DATASUBJ-1	Service enablers MUST provide a mechanism to allow data subjects to learn about their privacy settings at any time and be able to re-express existing privacy preferences. **C1**
DATASUBJ-2	Data subjects MUST be able to temporarily change the original configuration of his/her privacy preferences **B1**
DATASUBJ-3	Data subjects MAY require notification of changes to their privacy settings **A7**
DATASUBJ-4	Data Subjects SHALL be able to use a pseudonym as an identity. **J6**

Table 3: High-Level Functional Requirements from Data Subjects

6.2.3 Requirements on Recipients of Personal Data

Label	Description
RECIPIENT-1	Recipients requiring access to personal data MUST be first authenticated **B3**
RECIPIENT-2	The level of detail of the information collected SHOULD not be greater than necessary for the purpose for which it is collected. (This is a variation of the EU directives since they do not discuss the granularity of collection). **F1**

Table 4: High Level Requirements on Recipients of Personal Data

6.3 Proxy Functions

6.3.1 WAP Proxies

Label	Description
PROXY-1	WAP proxies provide various functions on behalf of users. Some of these functions may have privacy implications. Proxy operation for such functions MUST be provided consistently with privacy-dependent preferences, agreements, and indications.
PROXY-2	WAP proxies acting as a cookie proxy for the user SHOULD provide the user with control over cookies per the "WAP HTTP State Management user interface" of [HTTPSM].
PROXY-3	WAP proxies providing the WAP Proxy-Based Redirect feature MUST provide the user with control over the feature operation per [PROXY]. **E1**
PROXY-4	WAP proxies that provide the user's network identity or any other personally identifiable information to origin servers in HTTP requests, MUST NOT provide that information if doing so was inconsistent with the user's privacy preferences, service agreements, or privacy-related legal requirements.

Table 5: Proxy Functions

6.3.2 Cookies

Label	Description
COOKIE-1	Whenever cookies are used, there MUST be clear and comprehensive information about their purpose. **[EU02] Article 5**

COOKIE-2	Whenever cookies are used, the data subject MUST be given the opportunity to refuse those. However, if the cookie is required for the sole purpose of facilitating transmission of a communication or where it is strictly necessary in order to provide an online service explicitly requested by the subscriber or user, then the user SHOULD the informed of the consequences of refusing the cookie. **[EU02] Article 5**
COOKIE-3	To avoid informing the user each time a cookie is used, the data subject MAY give his consent to cookie placement by default
COOKIE-4	Data Subjects SHOULD be able to manage, (view, remove etc…) cookies on their device as well as at the proxy.

Table 6: Cookies

6.4 Location Information

Privacy requirements specific to Location enablers using the Privacy Checking Protocol can be found in [PCP].

The following requirements apply to service enablers that collect personal data related to the data subject's location: -

Label	Description
LOC-1	Service enablers MUST provide a mechanism to anonymise location data, and data from where a data subject's location can be extracted. Note: Anonymity of location data is required unless the data subject's consent is received for it's processing according to the purpose of providing a value-added service.
LOC-2	If location data is used for value added services, the system MUST have capabilities for informing the end user and obtaining her consent about this prior to the processing. **[EU02] Article 9**
LOC-3	Even where consent has been given, users and subscribers MUST continue to have the possibility, using a simple means with no additional charge, for temporarily refusing the processing of such data for each connection to the network or each transmission. **[EU02] Article 9**

Table 7: Location Information Requirements

6.5 Security

Label	Description
SEC-1	Personal Data on an individual may be stored in different places and accessible to applications or service enablers, e.g. a Location or Presence server. OMA must ensure that access and use of personal data SHALL be supported in a secure manner, i.e. to prevent data exchanged between authorised parties from being used fraudulently or being abused by authenticated or unauthenticated entities. Various technologies could be employed by service enablers to do this, for instance transaction logs, user names/passwords.

Table 8: High Level Security Requirements

OMA service enablers shall ensure that mechanisms are in place to ensure compliance to the following minimum set of security requirements: -

6.5.1 Authorisation

Label	Description
AUTHOR-1	Only recipients who are authenticated SHALL be authorised to receive personal data.
AUTHOR-2	Transaction logs MAY serve as legal authorization as required by different administrations. **A5**

Table 9: Authorisation Requirements

6.5.2 Authentication

Label	Description
AUTHENT-1	Data subjects SHALL be first authenticated and authorised by the controller (or processor on behalf of the controller) as trusted parties before being allowed to change privacy preferences
AUTHENT-2	Content providers MUST be authenticated by the service provider before being allowed to receive personal data **D3**
AUTHENT-3	A rules change transaction SHALL require authentication of the controller **A8**

Table 10: Authentication Requirements

6.5.3 Integrity Protection

Label	Description
INTEG-1	Personal Data in transit, storage and under processing MUST be protected against security attacks (e.g., eavesdropping, tampering, and replay attacks)
INTEG-2	A rules change transaction SHALL require adequate security **A9**
INTEG-3	When data is kept for statistical, historical or scientific purposes it SHOULD be anonymized. **[EU95] Article 6**
INTEG-4	Personal data that is removed from the system on the data subject's request MUST be completely erased. **[EU95] Article 14, 15**

Table 11: Integrity Protection Requirements

6.6 Charging

None identified

6.7 Administration and configuration

Requirements related to user administration and configuration of privacy preferences is found in section 6.2.2, in addition to the following: -

Label	Description
ADMIN-1	Service enablers that provide user access to their privacy preferences SHOULD permit such access from both mobile and wire line devices.
ADMIN-2	Service enablers SHOULD allow users to apply a default privacy preference profile and extend them to new services.

ADMIN-3	Where some granularity to privacy preferences associated with Personal Data exists, the Data Subject MAY be allowed to express a higher or lower priority to some privacy preferences compared to others.

Table 12: Administration & Configuration Requirements

6.8 Terminal devices and smartcards

Label	Description
TERM-1	Privacy preferences SHOULD be manageable on an identity basis, i.e. specific to a data subject. This will allow the privacy preferences of a data subject to be preserved when he/she shares devices e.g. by switching their SIM/USIM between devices or by using a multi-user device**. G1**

Table 13: Terminal Devices & Smartcards Requirements

6.9 Platforms

Not applicable.

6.10 Network interfaces

Label	Description
NI-1	A mapping between network specific information and application layer SHALL be provided to allow privacy settings to be to be set consistently. So, in the case of multiple networks, the same setting, as perceived by the user, would apply across all networks even though it was called differently in each network. **A6**
NI-2	Access to intercepted personal data in transit between controllers/processors and recipients SHALL be possible as required by Law Enforcement Agencies

Table 14: Network Interface Requirements

6.11 Usability

Label	Description
USAB-1	Mobile device users SHOULD be presented with unobtrusive and easy to use interfaces to their privacy controls **D1**
USAB-2	Access to intercepted personal data in transit between controllers/processors and recipients SHALL be possible as required by Law Enforcement Agencies

Table 15: Usability Requirements

6.12 Interoperability

None identified

7. Privacy Exceptions (Normative)

Label	Description
EXCEPT-1	There might be obligations under applicable laws in different jurisdictions that might be in conflict with, and sometimes override, obligations under privacy law (for example mandatory obligations to enable lawful interception). Those conflicting and/or contradicting obligations MUST also be taken into account.

Table 16: Privacy Exceptions

8. Privacy Guidelines Derived from Legal Directives (Informative)

The different aspects of informational privacy that need to be considered most often refers to the requirements placed by [EU97] and [EU02]. This is an informative section containing business practices that do not have a relationship to the technical work of OMA but could be enforced as legislative driven policy.

Meeting all the requirements from [EU97] and [EU02] is NOT absolutely necessary, but OMA service enablers are required to consider the following as a minimum set required to meet legal obligations.

8.1 Legitimacy

Principle: Personal data collection and processing is only admissible if permitted by legal provisions (in particular, where the processing is necessary for the purposes of performing a contract to which the data subject is a party or for taking steps at the request of the data subject prior to conclusion of such a contract) or if the data subject has consented. The only party able to decide how to use the personal data (give his/her consent) is the identified data subject him/herself. In particular,

All personal data collected SHOULD have an associated means to allow the controller/processor to avoid storing the personal data longer than that determined by the purpose for which was collected **[EU95] Article 6**

Processing of personal data that treats racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life MUST be avoided unless the data subject gives her explicit consent. **[EU95] Article 8**

8.2 Purpose specification and purpose binding

Principle: Personal data must be obtained for specified and legitimate purposes and should not be used for other purposes. In particular,

- All Personal data collected SHOULD have an associated binding which can be used to inform the data subject of the purpose its processing
- Traffic data that forms part of personal data MAY be used for billing purposes or for the purposes of marketing electronic communications services or value added services, for which the user has given consent
- Traffic data that forms part of personal data MUST be erased or made anonymous when no longer needed for the above purposes to which the user has given consent.
- If traffic data that forms part of personal data is used for billing purposes, the data subject MUST be informed about the type of data used, and the duration of the storage and/or processing.
- If traffic data that forms part of personal data is used for marketing or value added services, the system MUST have capabilities for informing the data subject and obtaining her consent about this prior to the processing. **[EU02] Article 6**

8.3 Transparency

Principle: The collection and processing of personal data shall only be allowed if it is necessary for the task. Services requiring processing of personal data SHOULD provide the data subject with an alternative, which involves less or no personal data. **[EU95] Article 7**

8.4 The data subject's right to correction, erasure or blocking of incorrect or illegally stored data

Service enablers that process personal data SHOULD provide a user interface, through which it is possible to add, remove and update the data once provided. Permissions, for example to send emails, SHOULD also be possible to alter. **[EU95] Article 12**

8.5 Security, confidentiality, integrity, and availability of personal data

Product developers SHOULD document what security mechanisms are being used to protect personal data **[EU02] Article 4**

9 Requirements not covered by this specification (Informative)

This document should be viewed as a minimum set of requirements for informational privacy on OMA architecture, i.e. to protect personal data, (in transit and storage) against unauthorised access and use, and to enable service providers to comply with a minimum level of applicable regulatory policies. However, the following aspects are not covered by this requirements document.

9.1 Protection from Unsolicited Messaging

OMA recognises the importance of protecting users from unauthorised access by applications or other people, e.g. being sent unwanted e-mails or push notifications. Protection against unsolicited messaging ("Territorial Privacy") is however considered outside the scope of this document because, except for content provider sharing of user information with third parties:

- The relationship between content providers and users, and content provider compliance with the terms of that relationship, are matters of the individual service
- Where no assumption of a content provider and user relationship exists, protection against unsolicited messaging is assumed to be provided at some point in the messaging path, e.g. as spam filters or firewalls

Such unsolicited message blocking measures as spam filters or firewalls, while important, are more appropriately provided by network security enablers.

Protection against "spam" is therefore not included in the aforementioned minimum set of regulatory policy requirements.

9.2 Handling Privacy in Different Jurisdictions

Most network operators usually only operate under the laws of a single jurisdiction, but there are scenarios where an operator's service platform connects to data networks in different countries and hence may serve individual users in different jurisdictions.

There is a fundamental legal problem of how the operator reconciles the privacy policies set by the various jurisdictions in question. There is the nationality of the subscriber, that of the subscription, that of the serving network, that of the home network and that of the application server to consider.

Although it is valid to consider that operators and service providers should meet the privacy requirements of those various jurisdictions, solutions to this problem are FFS. It is assumed that the policies that apply should be those of the jurisdiction where the service account of the subscriber is registered

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
n/a		

A.2 Draft/Candidate Version V.1.0 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-Privacy-V1.0	20030108	1, 2, 3, 4	First draft
	20030203	1, 2, 3, 4, 6	Changes to Title, Scope, Introduction, Requirements and Definitions (merge with agreed changes in OMA-REQ-2003-0062-Privacy_change request). Delete architecture figure and modify role diagram
	20030219	1,2,3,4, 6	Include changes to scope and introduction discussed at Long Beach TP. Include changes, additions to references and definitions contained in OMA-REQ-2003-0109
	200303012	1,2,3,4, 6 Create Annex A	Include changes to scope and introduction and requirements sections discussed on conference calls and Boston F2F meetings. Documents used; OMA-REQ-2003-0139, 0146, -0153, -0154,
	20030325	1,2,3,4, 6 create section 7	Grammatical changes to scope, introduction. Additions and corrections to Definitions and References and inclusion of diagram. Inclusion of legal exceptions section. Documents: OMA-REQ-2003-0161, -0162,- 0163 - 0205,
	20030428	2, 3.2, 7	Correction to document version name. Addition of URLs to references. Correction of error to note in 3.2 and modification to text in Clause 7, (as discussed in mail reflector)
	20030521	2, 3, 5, 6	Correction to document version name. List references and definitions alphabetically. Incorporation of privacy use cases contained in documents OMA-REQ-2003-0282, -0283, -0284 and –0285 together with the requirements from those. Incorporation of privacy related use case from the Proxy-based Re-direct Requirements Document together with the associated requirements. Addition of agreed changes from documents OMA-REQ-2003-0307, (including informative section on Spam protection). Incorporation of use cases from document OMA-REQ-2003-0300, together with the requirements from those. Incorporation of legal requirements from documents OMA-REQ-2003-0286, (Privacy Requirements based on the European Directive 95/46/EC) and OMA-REQ-2003-0299, (Privacy Requirements based on the European Directive 2002/58/EC).
	20030601	All	Corrections and re-arrangement of sections in previous versions. Addition of section on limits to the scope of the work (section 9); Move requirements derived from legislation into informative section on non-technical requirements.
	200306013	3, 6, 8, 9 Annex A	Corrections and additions made after OMA TP session Atlanta June 2003 and from documents OMA-REQ-2003-0379, -0383 and –0384
	20030625	6	Minor calrifications to sect. 6 and addition of requirement on Lawful Intercept interface.
	20030708	3, 4	Corrections and addition as per: OMA-REQ-2003-0491 (privacy roles) and OMA-REQ-2003-0492 (definitions) plus comments to those changes.

Document Identifier	Date	Sections	Description
	20030731	5, 6, 8	Corrections and addition as per: Use cases and requirements from OMA-REQ-2003-0436r2. Agreed changes to use cases and requirements from: OMA-REQ-2003-0474. 0475, 0476, 0477, 0478, 0479, 0480 and 0482
	20030817	3, 4	Corrections and addition as per: OMA-REQ-2003-0491 (privacy roles) and OMA-REQ-2003-0492 (definitions) plus comments to those changes.
	20030827	3.2, 4.1	Updated after e-mail exchange
	20031001	All	Updated after formal review during Berlin TP
Candidate Versions OMA-Privacy-V1.0.1	20061109		Updated after consistency review of Privacy 1.0 RRP
	20061122		Latest Template applied
	20061212	All	TP R&A OMA-TP-2006-0420R01

Appendix B. Text From EU Directives (Informative)

The following text extracted from the European legal directives is used as a basis for some of the requirements contained in this document. They have been reproduced by kind permission of the source, The European Union.

Disclaimer: Only European Community legislation printed in the public paper edition of the Official Journal of the European Union is deemed authentic.

B.1 Directive 95/46/EC

Article 6

Related Text

1. Member States shall provide that personal data must be:
(a) processed fairly and lawfully;
(b) collected for **specified, explicit and legitimate purposes** and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
(c) **adequate, relevant and not excessive** in relation to the purposes for which they are collected and/or further processed;
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
(e) kept in a form which **permits identification of data subjects for no longer than is necessary** for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

Article 7

Related Text

SECTION II
CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE

Member States shall provide that personal data may be processed only if:
(a) the data subject has **unambiguously given his consent**; or
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
(d) processing is necessary in order to protect the vital interests of the data subject; or
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

Article 8

Related Text

The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing **racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life**.
2. Paragraph 1 shall not apply where:
(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State

provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or
(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or
(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or
(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.
3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.
4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.
5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.
Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.
6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.
7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

Article 10

Related Text

Information in cases of collection of data from the data subject
Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:
(a) the identity of the controller and of his representative, if any;
(b) the purposes of the processing for which the data are intended;
(c) any further information such as
- the recipients or categories of recipients of the data,
- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
- the existence of the right of access to and the right to rectify the data concerning him
in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Article 11

Information where the data have not been obtained from the data subject:

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:
(a) the identity of the controller and of his representative, if any;
(b) the purposes of the processing;
(c) any further information such as
- the categories of data concerned,
- the recipients or categories of recipients,

- the existence of the right of access to and the right to rectify the data concerning him
in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.
2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

Article 12
Related Text

THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA

Article 12
Right of access
Member States shall guarantee every data subject the right to obtain from the controller:
(a) without constraint at reasonable intervals and without excessive delay or expense:
- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);
(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;
(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

Article 14 and 15

Related Text
SECTION VII
THE DATA SUBJECT'S RIGHT TO OBJECT

The data subject's right to object
Member States shall grant the data subject the right:
(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;
(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.
Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

Article 15
Automated individual decisions

1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.
2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:
(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his

legitimate interests, such as arrangements allowing him to put his point of view; or
(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

Article 16 and 17

Related Text

SECTION VIII
CONFIDENTIALITY AND SECURITY OF PROCESSING

Article 16
Confidentiality of processing
Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

Article 17
Security of processing
1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.
2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.
3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:
- the processor shall act only on instructions from the controller,
- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.
4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

B.2 Directive 2002/58/EC

Article 4

Related Text

Security

1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

Article 5

Related Text

Confidentiality of the communications

1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

2. Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.

3. Member States shall ensure that the use of electronic communications networks **to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller**. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

Article 6

Related Text

Traffic data

1. **Traffic data** relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service **must be erased or made anonymous** when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).

2. Traffic data necessary for the **purposes of** subscriber **billing** and interconnection payments **may be processed**. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

3. For the **purpose of marketing** electronic communications services or for the provision of **value added services**, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, **if the subscriber** or user to whom the data relate **has given his/her consent**. Users or subscribers shall be given the **possibility to withdraw** their consent for the processing of traffic data at any time.

4. The service provider must **inform the subscriber** or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3.

5. Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.

6. Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.

Article 7

Related Text

Itemised billing

1. Subscribers shall have the right to receive **non-itemised bills**.

2. Member States shall apply national provisions in order to reconcile the rights of subscribers receiving itemised bills with the right to privacy of calling users and called subscribers, for example by ensuring that sufficient alternative privacy enhancing methods of communications or payments are available to such users and subscribers.

Article 8

Related Text

Presentation and restriction of calling and connected line identification

1. Where presentation of calling line identification is offered, the service provider must **offer the calling user** the possibility, using a simple means and free of charge, of **preventing the presentation** of the calling **line identification on a per-call basis**. The calling subscriber must have this possibility on a per-line basis.

2. Where presentation of calling line identification is offered, the service provider must offer the **called subscriber** the possibility, using a simple means and free of charge for reasonable use of this function, **of preventing the presentation of the calling line identification** of incoming calls.

3. Where presentation of calling line identification is offered and where the calling line identification is presented prior to the call being established, the service provider must offer the called subscriber the possibility, using a simple means, of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling user or subscriber.

4. Where presentation of connected line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge, of preventing the presentation of the connected line identification to the calling user.

5. Paragraph 1 shall also apply with regard to calls to third countries originating in the Community. Paragraphs 2, 3 and 4 shall also apply to incoming calls originating in third countries.

6. Member States shall ensure that where presentation of calling and/or connected line identification is offered, the providers of publicly available electronic communications services inform the public thereof and of the possibilities set out in paragraphs 1, 2, 3 and 4.

Article 9

Related Text

Location data other than traffic data

1. Where **location data** other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such 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**. The service provider must **inform** the users or subscribers, **prior to obtaining their consent**, of the **type** of location data other than traffic data which will be processed, of the **purposes** and duration of the processing and whether the data will be transmitted to a **third party** for the purpose of providing the value added service. Users or subscribers shall be given the **possibility to withdraw their consent** for the processing of location data other than traffic data **at any time**.

2. Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

3. Processing of location data other than traffic data in accordance with paragraphs 1 and 2 must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service.

Article 11

Related Text

Automatic call forwarding

Member States shall ensure that any subscriber has the possibility, using a simple means and free of charge, of stopping automatic call forwarding by a third party to the subscriber's terminal.

Article 12

Related Text

Directories of subscribers

1. Member States shall ensure that **subscribers are informed**, free of charge and **before** they are **included** in the directory, about the **purpose(s)** of a **printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services**, in which their personal data can be included and of any further usage possibilities based on search functions embedded in electronic versions of the directory.

2. Member States shall ensure that subscribers are given the opportunity to determine whether their personal data are included in a public directory, and if so, which, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory, and to verify, correct or withdraw such data. Not being included in a public subscriber directory, verifying, correcting or withdrawing personal data from it shall be free of charge.

3. Member States may require that for any purpose of a public directory other than the search of contact details of persons on the basis of their name and, where necessary, a minimum of other identifiers, additional consent be asked of the subscribers.

4. Paragraphs 1 and 2 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to their entry in public directories are sufficiently protected.

Article 13

Related Text

Unsolicited communications

1. The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.

2. Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar components or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.

3. Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.

4. In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited.

5. Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.