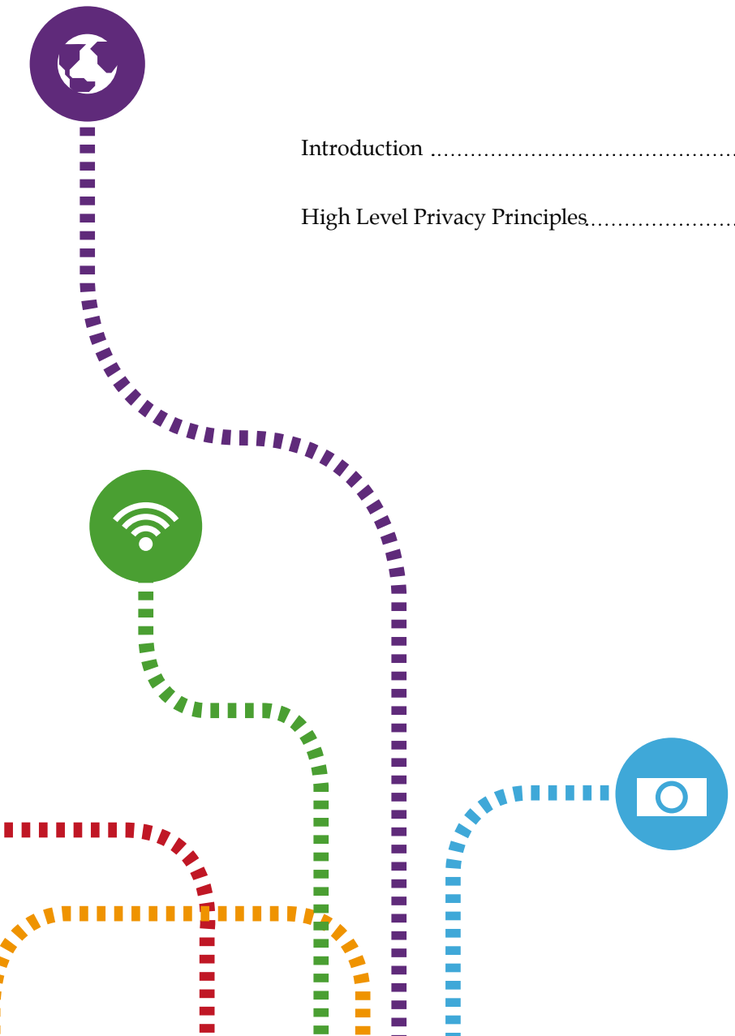
Mobile Privacy Principles

Discussion Document: Promoting a user-centric privacy framework for the mobile ecosystem

Version 1.0

Contents



Introduction

The mobile and web industries are in a process of unprecedented convergence. We are seeing the continuing innovation and rapid emergence of new social media and applications, many of which are being used across a multiplicity of networks and always-on Internet-enabled devices. These developments bring enormous economic and social value to individuals and to society as a whole. They also increasingly enable individual users to shape and present rich and personal identities online while bringing virtual communities of their choice literally in to the palm of their hands.

A critical factor for the sustainable development of this eco-system is a robust and effective framework for the protection of privacy, where users can continue to have confidence and trust in mobile applications and services. The mobile industry has a key opportunity to create and promote the conditions that ensure privacy is not only safeguarded throughout this eco-system, but also enhanced as an enabling platform for personal connectivity, presence and identity management.

Legal frameworks have been created in many parts of the world to address privacy and data protection concerns. These laws often vary from country to country. In a rapidly evolving and globally connected information society, this presents a continuing challenge as online and mobile service providers seek to comprehend and comply with myriad national legal requirements, while at the same time seeking to meet users' privacy expectations. These expectations increasingly transcend geographically bound legal frameworks as users seek consistent treatment of their privacy. Industry should play a pivotal role in creating consistent privacy standards and codes based upon internationally agreed principles that meaningfully protect the privacy of mobile users.

While not replacing applicable laws and regulations where they exist, this initiative is the start of a process that will seek to shape the way privacy is advanced, managed and protected across the emerging mobile eco-system. This process must involve a wide community of participants, including a variety of industry players, regulators, civil society and consumer representatives.

Framework for mobile privacy – 'Privacy Outcomes'

The objective of this initiative is to create a framework that identifies in broad terms the privacy standards that mobile users can expect from the wide range of applications and services that they use, i.e. the 'privacy outcomes'. These privacy outcomes should reflect commonly accepted privacy principles set out in international instruments and guidelines on privacy and data protection. The foundational principles below, based on these international instruments and guidelines, describe in high–level terms what these outcomes should be in a mobile context.

Codes and standards – 'Privacy by Design'

It is intended that the privacy principles adopted in this document, will act as a framework, informing separate standards and codes to address specific privacy issues, such as 'location privacy', transparency, notice and choice mechanisms. Such codes or standards should identify proportionate and effective measures to ensure that mobile users' privacy is protected, either in general or in specific contexts or service scenarios.

These codes or standards will seek to adopt a 'Privacy by Design' approach, and will seek to ensure these approaches are as consistent and harmonised as far as possible across mobile services and applications, so that both industry stakeholders and users become familiar with how privacy can be managed.

Privacy principles

The principles set out in this document broadly describe the privacy outcomes mobile users should experience. They are not intended to replace or supersede applicable law, but are based on recognised and internationally accepted principles on privacy and data protection. The key overarching objective of these principles is to foster business practices and standards that deliver meaningful transparency, notice, choice and control for users with regards to their personal information and the safeguarding of their privacy.

What do these principles apply to?

The principles apply to applications and services that may impact a user's privacy. This includes applications or services that seek to access, collect and otherwise use personal information and other private data about users which may be held on a mobile handset or which information may be generated by the end users use of a mobile application or service. They also apply to activities that impact user privacy in other ways, such as through intrusion, unwarranted contact or real–time monitoring.

Who do these principles apply to?

The privacy of mobile users is impacted by a number of factors. In many cases, a user's privacy will be primarily impacted by the collection, use or disclosure of personal information about them. This will often be by the person or organisation providing the relevant service or application. But other factors may be involved, such as the default settings or controls provided within an application, the prompts the user receives when installing applications or using certain features, and the way data about the user is made available to other applications or services.

Different stakeholders, such as the relevant service or application provider, the mobile operator, the handset manufacturer and the operating system or other software provider, will often control these factors, but even other users can have an impact, particularly within social media applications.

Each of these industry stakeholders should bear some responsibility for achieving the desired privacy outcomes for mobile users. We use the generic term 'responsible person' to refer to these stakeholders, and it is to them that these principles apply.

Some terms used in this document

Personal information – Personal information can mean many things to many people in the 'online' world, and has various meanings defined in law. This document does not seek to reinterpret the law. But when we use the term personal information in these principles, we intend it to include (but not limit to) the following types of information that relate to a mobile user and their use of mobile applications and services and information which may be considered private by users even though it may not be strictly protected in law:

a. Any data that is collected directly from a user (e.g. entered by the user via an application's user interface and which may include name and address, credit card details)
b. Any data about a user that is gathered indirectly (e.g. mobile phone number, email address, name, gender, birth data, location data, IP address, IMEI, unique phone ID)
c. Any data about a user's behaviour (e.g. location data, service and product use data, website visits)
d. Any user-generated data held on a user's device (call logs, messages, user-generated images, contact lists or address books, notes, and security credentials)

User – When we refer to the user, we generally mean the end user of the mobile device who initiates the use of an application or service, and who may or may not be the 'customer' of an application or service provider.

High Level Privacy Principles

Openness, Transparency and Notice

Responsible persons shall be open and honest with users and will ensure users are provided with clear, prominent and timely information regarding their identity and data privacy practices. Users shall be provided with information about persons collecting personal information about them, the purposes of an application or service, and about the access, collection, sharing and further use of a users' personal information, including to whom their personal information may be disclosed, enabling users to make informed decisions about whether to use a mobile application or service.

Purpose & Use

The access, collection, sharing, disclosure and further use of users' personal information shall be limited to meeting legitimate business purposes, such as providing applications or services as requested by users, or to otherwise meet legal obligations.

User Choice and Control

Users shall be given opportunities to exercise meaningful choice, and control over their personal information

Data Minimisation and Retention

Only the minimum personal information necessary to meet legitimate business purposes and to deliver, provision, maintain or develop applications and services should be collected and otherwise accessed and used. Personal information must not be kept for longer than is necessary for those legitimate business purposes or to meet legal obligations and should subsequently be deleted or rendered anonymous.

Respect User Rights

Users should be provided with information about, and an easy means to exercise, their rights over the use of their personal information.

Security

Personal information must be protected, using reasonable safeguards appropriate to the sensitivity of the information.

Education

Users should be provided with information about privacy and security issues and ways to manage and protect their privacy.

Children & Adolescents

An application or service that is directed at children and adolescents should ensure that the collection, access and use of personal information is appropriate in all given circumstances and compatible with national law.

Accountability & Enforcement

All responsible persons are accountable for ensuring these principles are met.

GSMA Head Office
7th Floor, 5 New Street Square, New Fetter Lane, London, EC4A 3BF, UK
Tel: +44 (0)207 356 0600

Further Information
mobileprivacy@gsm.org

www.gsmworld.com/mobileprivacy