Mobile Privacy Principles

Promoting consumer privacy in the mobile ecosystem

About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 250 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai and the Mobile 360 Series conferences.

For more information, please visit the GSMA corporate website at www.gsma.com

Follow the GSMA on Twitter: @GSMA

Introduction

The growth of the mobile internet, led by the success of smartphones and mobile broadband technology, continues to bring widespread benefits and opportunities to people around the world. However, it is also creating new challenges regarding the security and privacy of mobile users' personal information.

Research shows that mobile users are concerned about their privacy, wanting simple and clear choices to control the use of their information and the knowledge they can trust companies with their data. A lack of trust can act as a barrier to growth in economies that are increasingly data driven.

One of the major challenges faced by the growth of the mobile internet is that the security and privacy of consumers' personal information is regulated by a patchwork of geographically bound privacy regulations, while the mobile internet is, by definition, international. In addition, important categories of information such as location or traffic data are often only subject to privacy rules when processed by a mobile operator but not when processed by an internet content provider. This inconsistent applicability of rules is likely to be exacerbated as more devices and sensors are interconnected through the 'Internet of Things'.

This misalignment between national or market-sector privacy laws and global data flows makes it impossible for consumers' privacy expectations to be met in a consistent way by all the parties accessing their data. Equally, the misalignment distorts the market on data, causing legal uncertainty for operators, which can deter investment and innovation.

Mobile Industry Position

The wide range of services available through mobile devices offers varying degrees of privacy protection. To give consumers confidence that their personal data is being properly protected, irrespective of service or device, a consistent level of protection must be provided. The necessary safeguards should derive from a combination of internationally agreed approaches, national legislation and industry action.

Governments should ensure legislation is technology neutral and that its rules are applied consistently to all players in the internet ecosystem. Because of the high level of innovation in mobile services, legislation should focus on the overall risk to an individual's privacy, rather than attempting to legislate for specific types of data. For example, legislation must deal with the risk to an individual arising from a range of different data types and contexts, rather than focusing on individual data types.

The mobile industry should ensure privacy risks are considered when designing new apps and services, and develop solutions that provide consumers with simple ways to understand their privacy choices and control their data. The GSMA is committed to working with stakeholders from across the mobile industry to develop a consistent approach to privacy protection and promote trust in mobile services.

The GSMA Mobile Privacy Principles

These principles were developed in 2011 and describe the way in which mobile consumers' privacy should be respected and protected when consumers use mobile applications and services that access, use or collect their personal information.

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 mobile users with regards to their personal information and the safeguarding of their privacy.

The principles also provide the basis for which the GSMA and its members develop further guidance in specific areas or context. For example, they laid the foundation for the *Privacy Design Guidelines for Mobile Application Development* (2012)[1], which articulate the Mobile Privacy Principles in more functional terms and are intended to help drive a more consistent approach to protecting user privacy across mobile platforms, applications and devices.

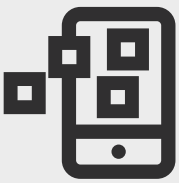
1. http://www.gsma.com/publicpolicy/privacy-design-guidelines-for-mobile-application-development. See also illustrative examples: http://www.gsma.com/publicpolicy/annex-of-illustrative-examples

MOBILE 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 AND 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 AND 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 AND ENFORCEMENT

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

What do these principles apply to?
The principles apply to applications and services that may impact a mobile 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 generated by their use of a mobile application or service. The principles 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, often controlled by multiple stakeholders. In many cases, a user's privacy will be primarily impacted by the collection, use or disclosure of their personal information. This will often be undertaken 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 a user receives when installing applications or using certain features, and the way data about that 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.

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:

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, address and 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 (e.g. 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.

The GSMA welcomes further collaboration and comments from across the mobile ecosystem and the broader ICT industry.

Please contact us at **mobileprivacy@gsma.com** or visit **www.gsma.com/mobileprivacy** for more information.

www.gsma.com/mobileprivacy

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London, EC4N 8AF,
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601