Mobile Connect Privacy Principles

Version 2.2

18 February 2015

Introduction

Mobile identity services play a key role in helping individuals establish and assert their identities online. Key to realising the potential economic and social benefits of mobile identity is establishing good privacy practices that foster trust and confidence among individuals.

These Principles are intended to guide the use of personal information in the provision of Mobile Connect identity services by Mobile Operators to 3rd Party Service Providers. The principles are 'user centred' and based on a common understanding that individuals have the right to expect that those who design, implement and operate identity services are committed to ensuring good privacy and security practices that respect and protect the privacy of individuals and the security of their data.

Mobile Connect services may include the simple authentication of a user via their mobile phone number and device, through to providing validated identity assertion and the sharing of user attributes. In the first step of Mobile Connect, when individuals are not on their operator's network they may be requested to provide their mobile phone number in order for them to receive an authentication prompt on their device from their Mobile Operator. This information is only processed and used for redirecting to the individual's Mobile Operator and is not stored nor shared with a Service Provider. Where there is a need for a greater level of assurance about an individual they may also be asked to enter a personal code.

The user's Mobile Operator will not disclose mobile numbers but will supply the Service Provider with a unique customer reference. This is to protect an individual's privacy and help them privately log-in to online services from any device without disclosing their mobile numbers or any other personal information until they choose to. Mobile Connect is about placing individuals and their mobiles at the heart of identity services and let them control when, how or if they wish to expose their real identities.

These principles are jurisdictional and technology neutral. They 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 encourage and establish **business practices and standards that** enable innovation but still **respect and protect privacy** through providing meaningful transparency, notice, choice and control for individuals over the use of their personal information.

Who the Principles apply to

The Principles apply to the processing of personal information by Mobile Operators and 3rd Party Service Providers ('Participating Organisations') in the provision of Mobile Connect branded identity services under the GSMA's Mobile Connect programme. The Principles are binding on Participating Organisations.

➢ Principle 1. Openness, Transparency and Notice

Mobile Operators and 3rd Party Service Providers shall be open and honest with users about the use of their personal information, and shall provide individuals with privacy notices that are clear, simple and prominent, and that aid comprehension and help users make informed choices.

A *privacy notice*, must as a minimum explain:

- the identity of the Participating Organisation responsible for any personal information collected and used
- where it is not obvious, the main purposes for which the individual's personal information will be used
- where it is not obvious, who personal information will be shared with and why
- whether the provision/collection of personal information is voluntary or mandatory (and if so, why)

Notices must be rendered in device appropriate ways (e.g. when accessed via a mobile device, laptop, tablet).

Each Participating Organisation must provide a hyperlink to a more detailed *privacy policy* that also describes the purposes of Mobile Connect. This separate policy shall include:

- a brief and clear description of how Mobile Connect works, including the assigning of any pseudonymous identifiers
- what personal information is collected and shared in order to provide Mobile Connect services requested by an individual (if this is not obvious)
- what personal information will be retained and for how long
- how individuals can contact the Participating Organisation with data protection and privacy enquiries
- the rights of individuals with regards the use of their personal information and how they can exercise these (for example, to obtain a copy of personal information held about them)

➢ Principle 2. Purpose and Use Limitations

Participating Organisations who collect and use personal information for the purposes of providing identity services shall limit the collection and use of data to that necessary to provide such services, or where otherwise necessary to meet legal obligations.

Any secondary uses of personal information that are incompatible with the provision and management of the Mobile Connect service shall take place only with an individual's Active Consent.

➢ Principle 3. User Choice and Control

Participating organisations shall provide individuals with opportunities to exercise meaningful choice, and control over the use of their personal information.

➢ Principle 4. Data Minimisation and Retention

The data collected and retained shall be reasonable, proportionate, and necessary for the purposes of providing Mobile Connect services.

Personal information may be retained and used only as long as necessary for those purposes, to fulfil audit requirements or to meet legal obligations. Data shall be deleted or rendered anonymous when no longer necessary to meet these requirements.

➢ Principle 5. Data Quality

Personal data shall be relevant and adequate for the purposes for which it's collected and used, and should be accurate, complete, and kept up to date. Measures shall be taken to ensure the integrity and availability of personal information.

Individuals shall be given the means to update their personal information, free of charge and in a simple manner.

➢ Principle 6. Respect User Rights – Individual Participation

Users shall be provided with information about their rights over the use of their personal information and shall be given an easy means to exercise such rights. These include:

- how to obtain a copy of any personal information held by a company, within a reasonable timescale
- how to have personal information that is inaccurate, or no longer justified, corrected or erased
- how to report and have complaints resolved regarding the processing of their personal information

➢ Principle 7. Security

Personal information must be protected, using reasonable safeguards appropriate to the sensitivity of the information, against risks such as loss, unauthorised access, destruction, use, modification, and disclosure.

Personal information shall be secure when at rest and in transit.

As part of the Mobile Connect service, a Mobile Operator will replace an individual's mobile number (Mobile Subscriber Integrated Services Digital Network-Number – MSISDN) with a unique identifier such as a Pseudonymous Customer Reference (PCR - identifier) in order to protect the privacy of an individual seeking to authenticate and access the services of a 3rd party service provider. This identifier must be unique to each service provider and sufficiently secured to prevent against the unauthorized re-identification of the end user's MSISDN.

Participating organisations may only re-identify an individual MSISDN under the following exceptions:

i. with an individual's Active Consent
ii. to provide a service requested by an individual, for the performance of a contract or to assist in the resolution of customer enquiries
iii. where required by law (e.g. a court order or other mandatory obligation)

Participating organisations shall establish policies and procedures for investigating and managing security breaches.

➢ Principle 8. Education

Where Participating Organisations directly provide Mobile Connect branded services they shall provide information about how the services work and ways for individuals to manage and protect their privacy.

Participating organisations shall establish internal programmes to educate employees on data protection and privacy requirements and to foster a culture of privacy.

➢ Principle 9. Children and Adolescents

Children and young people may lack the maturity to fully understand the implications of revealing their personal information or allowing others to collect and use it. Services directed at, or intended for, children and young people shall ensure that the collection and use of personal information is appropriate in all given circumstances and must at all times comply with national laws and any special legal requirements, including age verification laws.

Such services must use language and style that helps children and young people easily understand what is being asked and that helps them make informed decisions about the use of their data.

Principle 10. Accountability and Enforcement

All participating organisations are accountable for complying with these principles.

As a minimum, organisations shall:

- nominate a person to be responsible for ensuring compliance with these principles
- establish policies, procedures and practices, oversight and redress and the means for remediation of non-compliances

Definitions and terms:

Active Consent: means an individual is given a clear and prominent opportunity to agree a specific and notified use of their personal information.

Personal Information: includes, but is not limited to data that could be used to identify, locate or contact an individual. Personal Information may include:

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

Pseudonymous Customer Reference (PCR)[1]: is a unique identifier that replaces an individual's MSISDN and that may be used to distinguish one individual from another. Participating Organisations may only re-identify an individual MSISDN under the exceptions listed in Principle 7.

1 A PCR is used during Step 1 of Mobile Connect to uniquely authenticate an individual and map them to specific service provider accounts without revealing their identity and without individual's being required to disclose personal information. The PCR allows individuals to remain anonymous to participating organisations until such time that specific actions are taken to directly identify individuals by association to the PCR. In simple terms, the PCR is assigned and used to recognise but not identify individual users.