GSMA Mobile Privacy Design Guidelines

W3C Privacy and User Centric Controls Workshop

21 November 2014

GSMA Brief Introduction

The GSMA represents the interests of mobile operators worldwide. Spanning more than 220 countries, the GSMA unites nearly 800 of the world's mobile operators, as well as more than 230 companies in the broader mobile ecosystem.

GSMA Key Initiatives:

- Members including handset and device makers, software companies, equipment providers and Internet companies, as well as organisations in financial, healthcare, media, transport and utilities sectors. (e.g. Samsung, Facebook, Qualcomm)
- Areas of focus include:
  - Fraud & Security
  - Spectrum
  - M4D
- Key Events: Mobile World Congress, Mobile Asia Expo, Mobile 360, Connected Women

Mobile privacy: complex ecosystem

GSMA Mobile Privacy Initiative

- Established in 2010
- The **Key Objective**: Identify mobile friendly methods for users to make informed decisions about their privacy and the use of their personal information
- Address key mobile privacy challenges as an *industry*
- Published GSMA Mobile Privacy Principles
- Published GSMA Privacy Design Guidelines for Mobile Applications (Feb 2012)
- Published ‘Accountability Framework’
- Conducted Consumer Research

GSMA Privacy Design Guidelines Main Points

- **Harmonise approaches** to privacy across platforms, applications and devices, fostering the development of a common set of functional requirements;

- Enable mobile users to benefit from a **consistent functional treatment of** their **privacy across platforms and devices**, strengthen their awareness and help them make decisions relevant to their interests and contexts;

- **Encourage innovation** in the development of privacy controls;

- **Establish a framework** of confidence and trust in the mobile ecosystem, and make it easier for developers to build in privacy from the outset.

Mobile Privacy Design Guidelines Key Areas

- Draw from a number of existing privacy frameworks
- Provide an overall framework to help develop more detailed privacy design guidelines and codes of conduct and business practices

Openness, Transparency & Notice

Purpose & use

User Choice & Control

Data Minimization & Retention

Respect User Rights

Security

Education

Children & Adolescents

Accountability & Enforcement

Guidelines - content

Transparency, choice and control — putting the user first

A key aspect of fostering confidence and trust in applications is being open with users and letting them know:

- who's collecting and using their personal information
- why personal information is being used
- what personal information is being shared, with whom and for what purposes.

Users should have enough information to make an informed choice about whether to use an application and the consequences of doing so. Some of this information may be obvious before a user downloads or activates an application and so makes no additional disclosures about an application necessary.

In short:

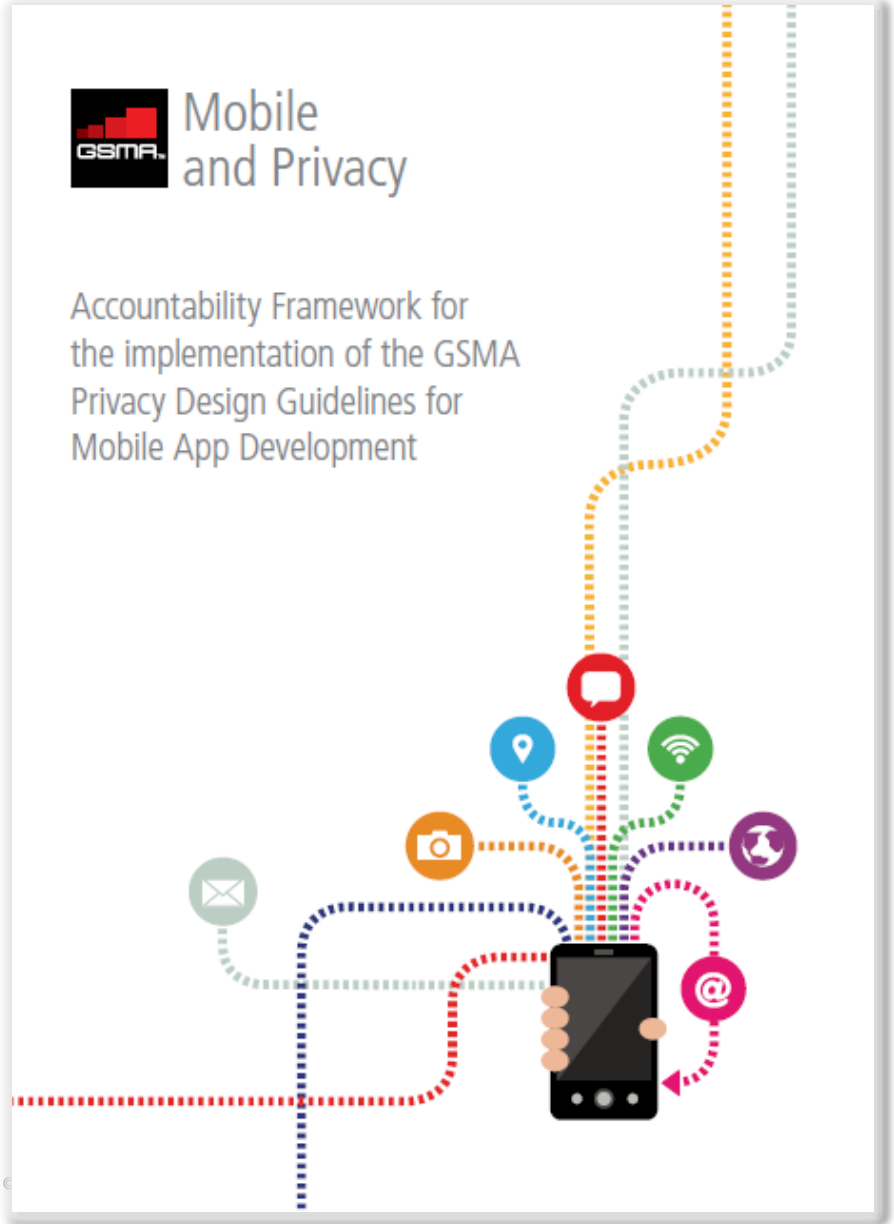
- **Be transparent:** Tell users who you are, what personal information you require, what you intend to do with it and who you intend to share it with (and why!) — but don't overburden them with prompts!
- **Help users manage their privacy:** Make them aware of an application's privacy default settings.
- **Give users easy to understand choices and mechanisms for managing their privacy:** Make it easy not hard — they'll like you better for it.

Guideline	Implementation	Use case and examples
TCC1 **Do not surreptitiously access or collect personal information.** An application must not secretly access and collect personal information about users.	Before a user downloads or activates an application, he or she must be presented with information about: • what personal information an application will access, collect and use • what personal information will be stored (on the device and remotely) • what personal information will be shared, with whom it will be shared • and for what purpose	An application must not access a user's location if the application isn't a location based service app. If location data is secondary to the app and needed to meet other commercial objectives then you need to get a user's active consent (see the 'location privacy' section below). An application must not access and use contact details held in a device's address book unless this is part of the apps functionality clearly explained to

4

GSMA Privacy Design Guidelines for Mobile Applications

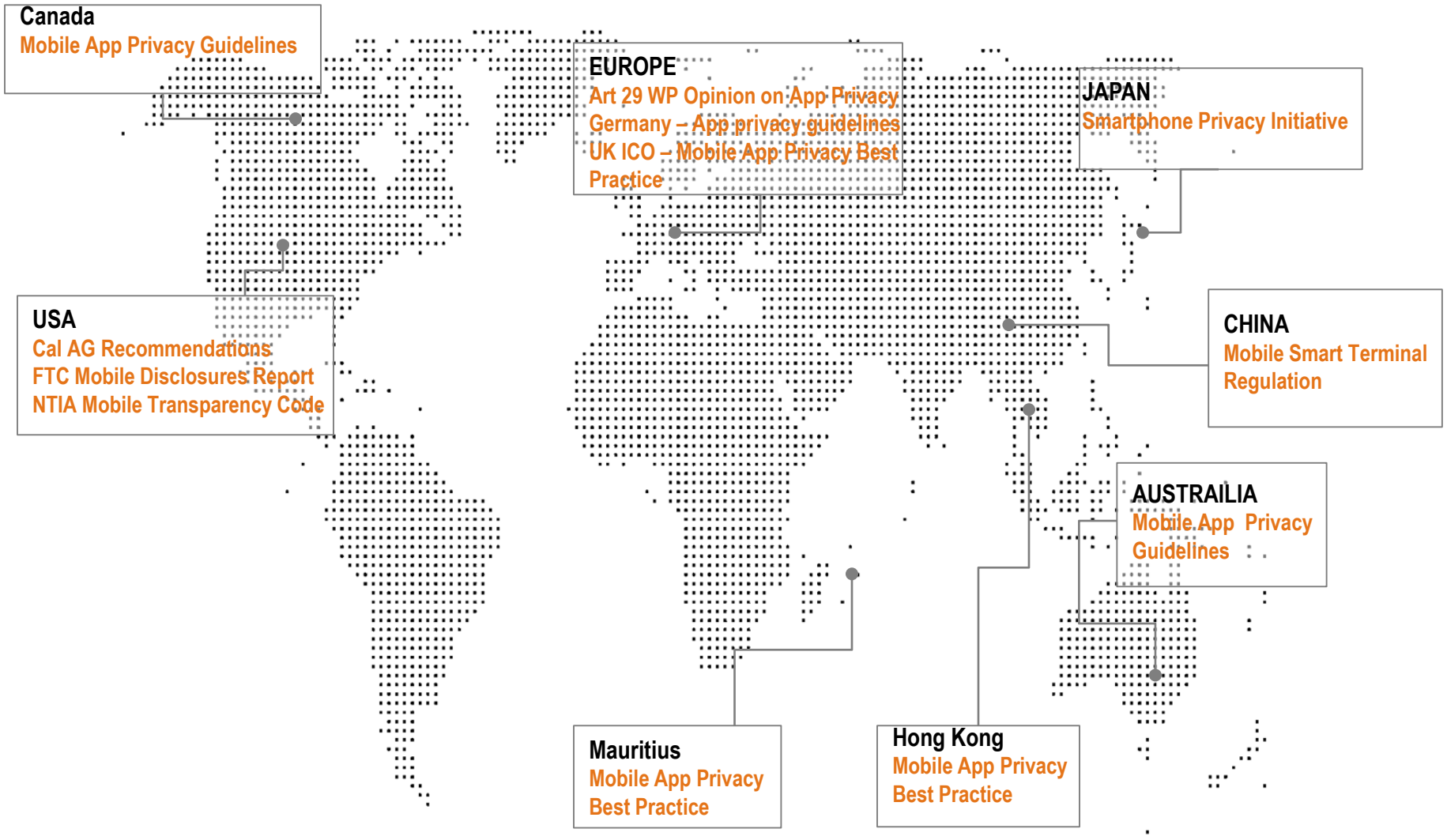
Establishing Accountability



Key objectives:

- To help organizations to demonstrate that their business practices comply with the Guidelines
- To be applicable across different international regions of operations
- To help foster the confidence and trust if customer and other stakeholders

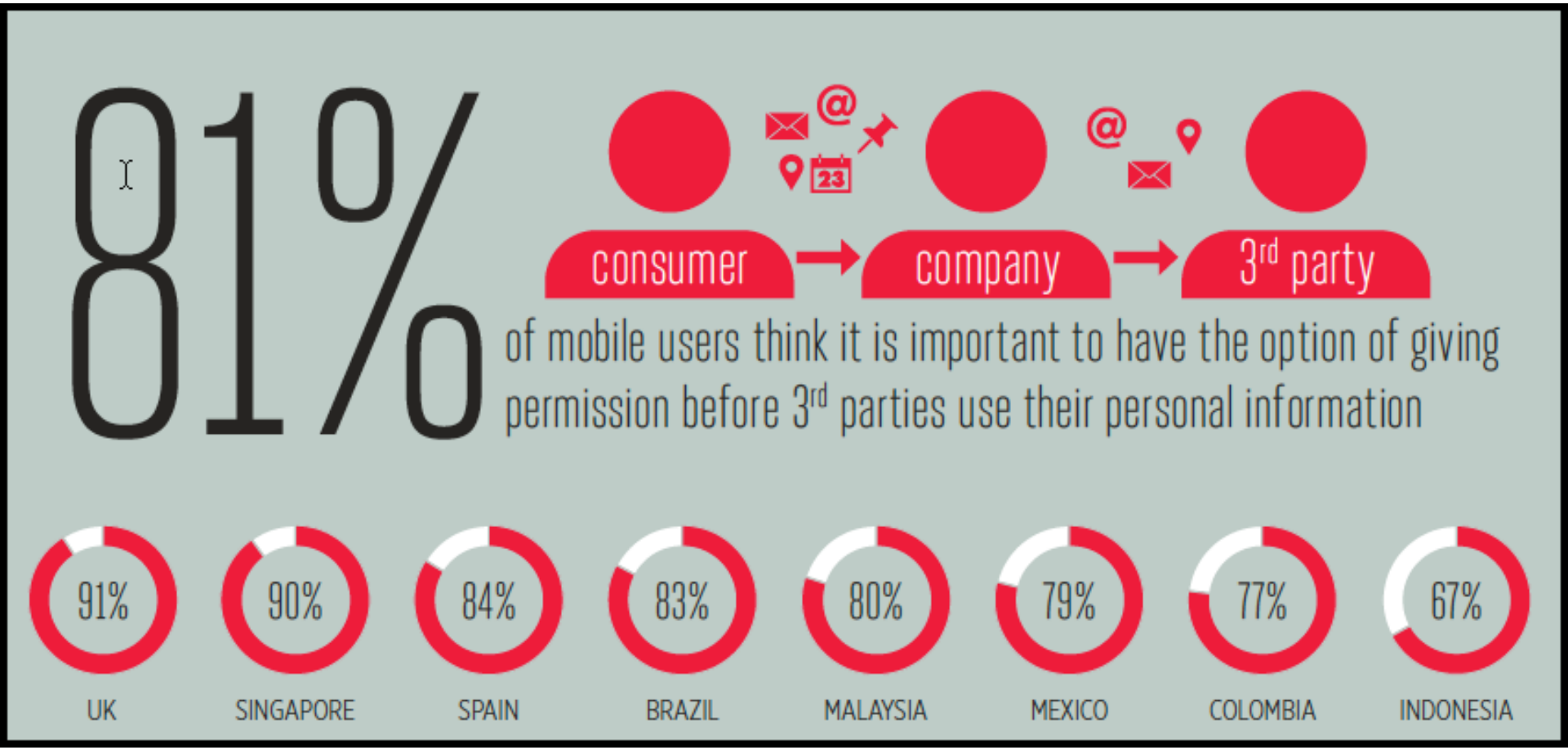
International Mobile Privacy developments

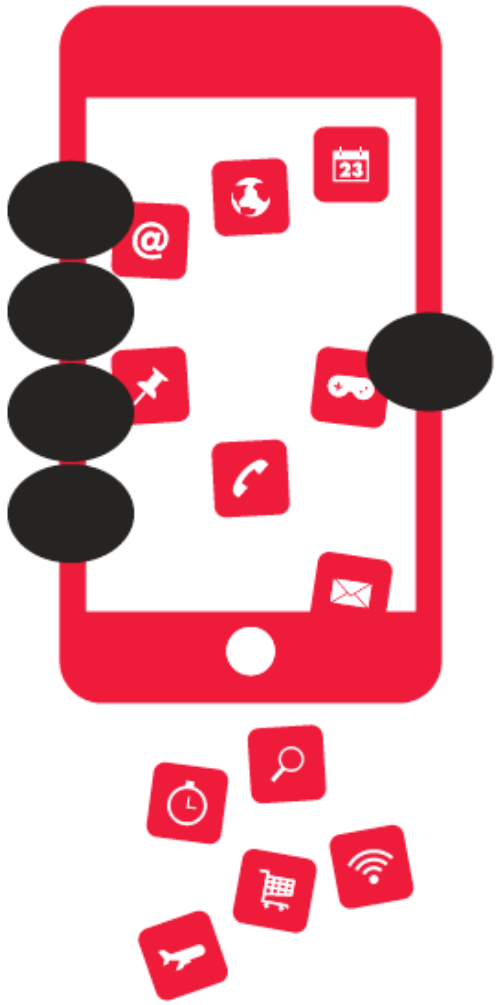


Source: QUALCOMM

BACKUP

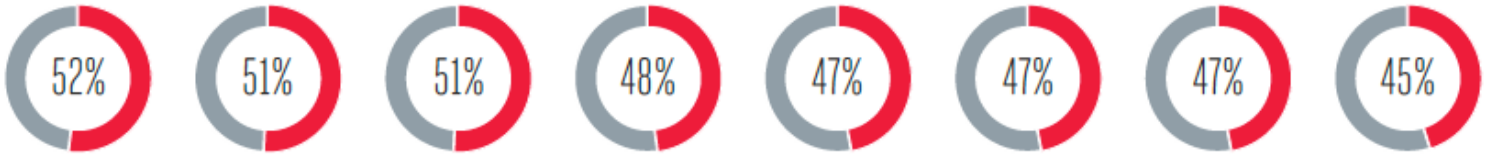
It's more than the law: Privacy Matters –designing for trust





48%

of mobile app users with privacy concerns would limit their use of apps unless they felt sure their personal information was better safeguarded



60%

of mobile users want a consistent set of rules to apply to any company accessing their location, regardless of how they obtain this information