



GSMA Position Paper for the W3C workshop on Privacy for Advanced APIs

Submitted by Patrick Walshe, Government and Regulatory Affairs, GSMA.

### **W3C Workshop background – Privacy for Advanced Web APIs**

As the Web advances toward becoming an application development platform that addresses needs previously met by native applications, work proceeds on APIs to access information that was previously not available to Web developers. The broad availability of possibly sensitive data collected through location sensors and other facilities in a Web browser is just one example of the broad new privacy challenges that the Web faces today.

[The] workshop serves to review experiences from recent design and deployment work on device APIs, and to investigate novel strategies toward better privacy protection on the Web that are effective and lead to benefits in the near term.

There is a need to establish participatory privacy and security dialogue with industry, civil society, regulators and other key stakeholders to develop and agree appropriate interoperable privacy standards, trust levels and mechanisms.”

### **Position Statement:**

The rapid convergence of the mobile and web industries, combined with the growth in powerful, sophisticated internet-enabled smartphones, new business models and innovative applications and services is re-shaping the privacy landscape and leading to the emergence of new privacy challenges across the mobile ecosystem.

Users of internet-enabled mobile handsets sit in an increasingly diverse, fragmented and complex (global) web of relationships with mobile operators, device manufacturers, browser and operating system vendors, application developers and ‘app stores’, search engine companies and advertisers, but do not appear to have consistent privacy experiences by which they can understand who has access to and use of their data, or by which they may exercise choice and control in differing contexts. Approaches to ‘privacy’ by these various entities are often based on ‘compliance’ with national and local law, specific business imperatives and challenges of building applications and services for a multiplicity of devices, networks and modalities. This reality may not necessarily meet the privacy interests, concerns and expectations of mobile users. User privacy interests and expectations increasingly transcend geographically bound laws and regulations as users seek consistent treatment of their privacy irrespective of technologies and business models, and who may wish to be actively engaged in the management of their privacy.

The GSMA is of the view that a ‘privacy by design’ approach is needed to establish a



‘user centric’ participatory privacy framework that can provide consistent user privacy experiences and choice wherever and whenever a user engages with services, which reflects user interests, which can drive confidence and trust in, and engagement with, applications and services, and which can continue to drive innovation in technology and business models.

**A user centric participatory privacy framework:**

The GSMA is currently seeking to establish a user centric participatory framework that is ‘outcomes’ focussed and which seeks to deliver context aware and device appropriate privacy experiences that drive awareness, and user-based, context appropriate opportunities for users to express choice and control over their personal information. This will require dialogue, collaboration and collective action among standards organisations, operators, web industries, device manufacturers, OS vendors, developer communities, regulatory bodies, and privacy and consumer interest organisations.

It is proposed the privacy framework is based on ‘**Privacy Principles**’ to provide an overall framework to guide the development of general rules setting business practice and standards that respect and protect the privacy of users and the security of their data. The Principles are open and framed at a high level to allow for broad application and flexibility, both across differing stakeholder groups and jurisdictions, and according to developing technological contexts and business models.

The Principles may support a number of ‘outcomes’ such as the development of user prompts, notice and choice mechanisms that provide context aware ‘privacy nudges’ and the development of privacy design guidelines. Privacy design guidelines are especially considered important given that current application security frameworks appear to treat privacy as a by-product of security, and which do not necessarily address that users have privacy interests, concerns and expectations that are being shaped by their interactions with the complex web of relationships touched upon above. Where privacy is explicitly considered in the design process, it not always done so consistently across platforms and standards entities. The consistent functional treatment of privacy between applications and across platforms will lead to greater awareness and familiarity among users regards the privacy implications of an application and the choices open to the user – this in turn will help enable users to manage their privacy according to their interests and expectations.

It is considered that Privacy Design Guidelines may help to express in functional terms the GSMA Privacy Principles, and could help to:

- foster a ‘privacy by design’ approach to help establish best practice to be followed by applications and services that seek to create, access and share a user’s personal information
- ensure applications and services respect user privacy and execute in ways that safeguard privacy and security of data



- drive consistent user privacy experiences and enable users to manage their privacy in effective ways
- establish common privacy criteria to support development of functional requirements for apps that can be applied across platforms and devices
- strengthen assurance across participants and stakeholders that privacy is being addressed in a consistent and collective manner
- modular in approach to address specific privacy issues (e.g. location privacy, children's privacy, social networking)
- reduce developer burdens and barriers caused by a fragmented environment
- engender a different way of thinking about privacy and drive a user-centric participatory privacy culture
- help inform policy decision making

**In closing:**

The development of policy and privacy standards relating to the 'web' are often borne out of users experiences and challenges from the fixed world. It is uncertain the degree to which such approaches will reflect the uniqueness of the mobile ecosystem and user interests, concerns and expectations. It is important to take a renewed approach to respecting user privacy and providing a privacy framework that provides real transparency and effective choices in a globally connected mobile world.

Mobile users may generate richer seams of data and create privacy tensions as they engage with contextually aware services and as they shape and present identities online from within the palm of their hand. It will be crucial to identify and establish appropriate privacy criteria and mechanisms that provide context-aware opportunities for users to manage their privacy in dynamic situations and relationships. Users must be placed at the heart of the design process. A key goal in today's globally connected mobile world must be to establish consistent user privacy experiences wherever and whenever a user engages with applications and services.

A copy of the GSMA's Mobile Privacy Principles is supplied with this position statement for consideration by the W3C.