GSMA response to the Preliminary FTC Staff Report "*Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policy Makers*"

16 February 2010

Patrick Walshe
Director of Privacy
GSMA
Seventh Floor
5 New Street Square
New Fetter Lane
London EC4A 3BF
UK

About the GSMA

The GSMA represents the interests of the worldwide mobile communications industry. Spanning 219 countries, the GSMA unites nearly 800 of the world's mobile operators, as well as more than 200 companies in the broader mobile ecosystem, including handset makers, software companies, equipment providers, Internet companies, and media and entertainment organisations. The GSMA is focused on innovating, incubating and creating new opportunities for its membership, all with the end goal of driving the growth of the mobile communications industry.

For more information on the GSMA, please visit: Mobile World Live, the new online portal for the mobile communications industry, at www.mobileworldlive.com and the GSMA corporate website at www.gsmworld.com. For specific information about the GSMA's consumer protection work please visit http://www.gsmworld.com/our-work/public-policy/protecting_consumers.htm

Executive Summary

The GSMA welcomes the opportunity to provide comment on the Federal Trade Commission's preliminary report on *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policy Makers*. While we are providing written "views" as outlined in this response, we believe the issues raised by the report are of such importance that the solutions sought by the Commission can only be found by facilitating multi-stakeholder dialogue and co-operation. The GSMA would welcome the opportunity to engage in such dialogue.

The proposed framework is a welcome and positive development and demonstrates the FTC's thoughtful leadership on the important issue of consumer privacy. The report recognises and seeks to address key issues and challenges emerging from a rapidly changing and converging online and mobile ecosystem and developments in technology, business models and information use. These developments have given rise to new categories of data that do not easily fall under definitions of 'personally identifiable information' or 'personal data' contained in existing legal frameworks. Such new categories of data may nonetheless hold significant privacy implications and other consequences for users. Likewise developments in abilities to collect, use, share, and profile information about consumers and their behaviour in real-time give rise to new concerns about transparency, notice and choice in ways that are fair and meaningful to users and which help them to manage their privacy in simple and effective ways while enjoying the benefits of more personalized services and offerings.

It is right that the Commission seeks to address these developments but we urge the Commission to do so in ways that address consumer privacy while fostering continuing innovation in technology, business models and information use. Such innovation has brought significant benefits to individuals and to society as a whole. It is important to establish a regulatory framework that facilitates continuing innovation and which supports technological and self-regulatory solutions to ensure consumer privacy is respected and protected by all players in what is a global interdependent ecosystem of technology and service providers, device manufacturers, app developers, advertisers, internet companies and others. Given the pace of developments in technology and business models we believe cross industry self-regulatory mechanisms are a more effective and responsive means of addressing specific technology driven privacy concerns and consumer interests.

The GSMA recently launched a mobile privacy initiative and a set of universal Mobile Privacy Principles[1] to address many of the key challenges outlined the Commission's report and to help establish and shape a culture of privacy that respects and protects the privacy of users across the mobile ecosystem. The GSMA has been working with its members and engaging with other players in the broader ICT ecosystem to consider the privacy challenges emerging in the mobile sector. A first step in the initiative has been to develop the mobile privacy principles that can be used as a framework to shape how privacy should be respected and protected when consumers use mobile

[1] http://www.gsmworld.com/our-work/public-policy/mobile_privacy.htm

[2] '*Informed Consent by Design*', Friedman, Lin and Miller. http://hornbeam.cs.ucl.ac.uk/hcs/teaching/GA10/lec9extra/ch24friedman.pdf

applications and services that access, collect and use their personal information.

The GSMA intends to use the privacy principles to develop more detailed guidelines and to help guide the development of clear and simple ways for customers to manage their information and their privacy on mobile phones. The principles are just a first step in a long journey but addressing mobile privacy is an ongoing challenge that requires the support and collaboration of the wider Internet industry, civil society and regulators, working together. The GSMA welcomes input on the privacy principles and encourages stakeholders from the broader ICT industry to join in conversation and partnership on this important work.

The GSMA also considers it important that any revised data privacy framework provides clarity and certainty for businesses and helps establish consistent privacy standards and expectations for consumers. Such consistency will help drive a 'privacy by design' approach among businesses across the ecosystem and help consumers become familiar with the privacy implications of applications and services and with ways to manage their privacy.

We also believe it is important to avoid viewing privacy in static terms in respect of providing transparency, notice and choice. We do not believe the Commission should prescribe the content and timeliness of notice and choice mechanisms. Privacy is dynamic and contextual – a user's privacy interests (expectations, needs, wants, concerns) reflect stages of development in relationships with companies and engagement with apps and services. It will be important to understand how business may meet these interests in clear and simple ways that are context and device appropriate and that enhances rather than undermines the user experience. The user experience is important in ensuring consumer engagement with applications and services and strengthening the success of a business. Any proposed regulatory framework must consider these legitimate concerns of business.

We should like to offer comments on three key areas of the proposed framework and to specific questions posed by the Commission: Scope, Privacy by Design, Consumer Choice and Transparency. Our response is restricted to comment on issues and challenges as they apply to the mobile ecosystem.

1. Scope.

The Commission is seeking to significantly broaden the scope of consumer privacy protection by applying the privacy framework to "consumer data that can be reasonably linked to a specific consumer, computer or device". We are generally supportive of this intention and recognise that new categories of data and new abilities to collect, profile, analyse and target consumers may hold privacy implications and other consequences for individuals even though they may not be identifiable from the data. The mobile phone is an inherently more personal device giving rise to richer more intimate data trails and profiles as consumers meet more of their personal, financial, entertainment, information, navigation and e-commerce needs via their mobile devices. It is right that this issue addressed.

We are however, concerned that the Commission has not sought to clarify what it considers 'consumer data' to be. This will be important in ensuring the Commission avoids an overly restrictive regime that stifles legitimate uses of data and also to meeting other goal of privacy by design and ensuring consumers truly can make informed decisions. For example, there are circumstances under which data need be linked to a mobile device identifier in order to render services in ways that are appropriate to the device, the screen or operating system. These legitimate needs must be considered in the Commissions review and should be properly considered via expert workshops.

2. **Privacy by design**. *Companies should promote consumer privacy throughout their organizations and at every stage of the development and ongoing lifecycle of their products and services.*

The concept of 'privacy by design' is not explored in great detail in the report. While we do not advocate prescribing the detail of 'privacy by design' in legal frameworks, we believe it would be helpful to clarify the concept and translate fundamental privacy principles into meaningful privacy design guidelines that can be implemented by all players in the mobile ecosystem. The report calls for industry to implement privacy practices systematically but does not consider what the 'industry' is or the complexity of achieving this in global terms. For example, the mobile 'industry' involved in providing services to mobile consumers includes mobile carriers, device manufacturers, mobile operating system (OS) vendors, chip manufacturers, browser vendors, search engine providers, social network providers, communications providers, platform providers, advertisers, app stores, and app developers. The various players are often interdependent of each other. It is clear that mobile users are becoming increasingly enmeshed in this complex and global web of relationships but without enjoying consistency in privacy experiences. The 'systematic' implementation of privacy by design will require a regulatory framework that incentivises pro-active co-operation and collaboration among ecosystem players to ensure a truly user centric approach.

The complexity of the online and mobile ecosystem and the global reach of apps and services call for consistency in approaches to privacy by design especially regards transparency, notice and choice. Users expect the consistent functional treatment of privacy between applications and across platforms and devices, and this will in our view lead to greater user confidence, trust and continued growth. A key challenge is to ensure privacy is considered in contextually aware and device appropriate ways to assist comprehension and effective exercise of informed choice and

preference[2]. This will involve handset manufacturers, OS vendors, app developers, browser vendors and advertisers to work together to meet the consumers' privacy interests by ensuring privacy' is designed in at the engineering level and not just adopted at a 'policy' level if the 'industry' is to deliver 'usable' transparency, notice and choice mechanisms for consumers.

Privacy by design also requires addressing the issue of accountability and responsibilities[3]. A key question and significant challenge is which parties in the value chain that provide an app or service and which parties participate directly or indirectly in the collection, use and sharing of 'consumer data' should be responsible for protecting the privacy of the consumer and the security and confidentiality of their data? As an example, consider the scenario where a mobile consumer in the UK downloads an app from an 'app store' located in the US, but where the app is developed and provide by a developer located in Africa or India. The developer may have entered into an agreement with a mobile media analytics company to insert code into the app in order to understand the users use of the app. The code may access, collect and use a mobile phone's Unique Device Identifier (UDID), location data, mobile number and/or a user's 'personal information' stored or cached on the device. That data may be transferred to third parties in other third countries with no formal data privacy legal frameworks. The data may be used to target the user with in-app or 'around' app advertising or to build up a persistent unique profile for other purposes. The app store may also access and use the UDID, location data and user data for purposes including behavioural advertising. All players in this scenario bear some responsibility for making the user aware of the intended uses of their data and for providing the user with transparent, clear and simple means to express preference and choice over such use, but practically speaking how can this responsibility be implemented? All players should be responsible for ensuring their products and information practices are designed with privacy in mind. Privacy by design requires that all players in the broader mobile ecosystem address these questions and challenges.

Other questions arise from the above scenario. How might an independent developer in Africa or India understand the complexities of law and 'privacy by design' of differing jurisdictions and industry approaches? Who should be responsible for the privacy practices of the app – the developer, the app store operating from the USA, the mobile media analytics company established in the USA? What if the app is provided online via an independent app store that is not located in the USA but accessible by consumers in the USA – how might good privacy practices be encouraged and enforced in these contexts? This latter consideration is important given that many application developers are located overseas and the views of some that 'apps' will take advantage of HTML5 developments and be accessed via the browser[4] rather than being downloaded to a mobile device as a 'native app'. HTML5 is in its infancy and the subject of concerns over privacy raised by the web

[2] '*Informed Consent by Design*', Friedman, Lin and Miller. http://hornbeam.cs.ucl.ac.uk/hcs/teaching/GA10/lec9extra/ch24friedman.pdf

[3] The Center for Information Policy Leadership and the 'accountability project'. The Centre recently hosted a meeting in Madrid to discuss how businesses may implement an accountability framework and also how regulators may incentivise accountability efforts. http://www.hunton.com/resources/sites/general.aspx?id=45

[4] Vic Gundotra, Google Engineering vice president. "We believe the web has won and over the next several years, the browser, for economic reasons almost, will become the platform that matters and certainly that's where Google is investing." July 2009, http://blogs.ft.com/fttechhub/2009/07/app-stores-are-not-the-future-says-google/

standards body W3C and respected academics[5] – how might privacy be designed into an emerging industry standard, who will set those standards and who will ensure accountability?

3. **Simplifying consumer choice**. *Companies should simplify consumer choice, and offer choice at a time and in a context in which the consumer is making a decision about his or her data, and not via lengthy legalistic privacy notices*.

The GSMA supports the commission's efforts to provide consumers with timely, simplified notices and choice mechanisms, moving away from legalistic, complex, lengthy privacy notices premised on static notions of privacy. Such legalistic notices do little to aid consumer awareness and comprehension in dynamic technology driven environments.

The Commission asks a number of questions regarding transparency, notice and choice. We should like to comment on these specific questions:

a. is the list of proposed 'commonly accepted practices' too broad or too narrow?

We welcome the Commissions intentions to clarify what it considers commonly accepted practices and to relax the requirement to obtain consent for commonly accepted practices such as fraud prevention and internal business operations. We are pleased to see recognition of the legitimate needs of business, especially first party marketing. We feel this list should be illustrative and not exhaustive in order to provide flexibility for new innovative and creative services.

However, we do feel further clarification is required in respect of first party marketing to ensure a business is not prevented from making it's customers aware of the products and services of partner organisations with whom it works. For example, a mobile carrier might work with handset manufacturers, OS vendors and social media organisations to design cell phones that meet the needs of specific consumer segments. The marketing of such cell phones and the social media and other apps will involve communicating information about the partners and their apps/services. Mobile carriers should be entitled to rely on the proposed 'first party marketing' provisions in such situations and not be required to secure additional consents. A failure to address this situation may result in confusion, uncertainty and negative impact on the commercial success of businesses as demonstrated by experiences in the EU where EU ePrivacy rules[6] restrict mobile carriers to marketing only their similar products and services. Recent research into the impact of privacy regulation on online advertising suggests that in Europe, privacy laws have reduced the effectiveness of banner advertising by 65% while increasing costs to business[7].

[5] *HTML5 Update: W3C Says Not Yet Viable, Privacy Concerns Raised* (http://www.cmswire.com/cms/web-cms/html5-update-w3c-says-not-yet-viable-privacy-concerns-raised-008941.php?pageNum=2) and *Privacy Issues of the W3C Geolocation API*, Nick Doty, Deirdre K. Mulligan and Erik Wilde, UC Berkeley http://escholarship.org/uc/item/0rp834wf#

[6] European Commission Directive 2002/58EC (to be replaced by Directive 2009/136EC). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML and http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:En:PDF

[7] Privacy Regulation and Online Advertising, Avi Goldfarb and Catherine Tucker. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600259

b. what is the most appropriate way to obtain consent for practices that do not fall within the 'commonly accepted' category?

We are concerned to learn that the Commission may automatically consider geolocation data as 'sensitive data'. We are concerned that the concept is not well defined in the document. We have particular concerns that the processing of 'geolocation data' will always require the 'affirmative express consent' of individuals. This approach fails to consider the dynamic and contextual nature of privacy and also seems at odds with the Commission's consideration of 'just in time notices'. We believe a more harms based approach is required to the issue of 'sensitive data'.

With regard to geolocation data, we believe the Commission should consider the active and passive nature of services that use and share the location of individuals and the fact that individuals are also actively engaged in the sharing of their location. We consider 'active location services' as those initiated directly by the user of a mobile phone or online service who is expressly asking to be located or who wishes to disclose their location information to others. As an example, a mobile user may find themselves outside the offices of the FTC and needing to locate the nearest ATM facility in order to obtain cash. This information will be requested from a commercial location based information service that may also combine navigation capabilities to help direct the user to the ATM. As the individual is asking to be located both at initiation and during the use of the service, we believe it unnecessary to require a company to obtain any additional 'affirmative express consent' of users in this context. Consent is implicit in the request. Requiring additional 'affirmative express consent' of users would require business to provide users with additional privacy notices and consent choices that may serve to burden the user without enhancing their privacy. This would also involve the diversion of financial and developmental resource that could be better expended on other privacy challenges. Affirmative express consent in an active location request scenario should be required only where there is an intention to use the individual's location data to target the individual or to share the data with third parties for secondary commercial purposes not linked to the original 'where's my nearest ATM' request.

Passive location services allow one user to locate or track another user once a specific service has been enabled. We believe these services hold significant privacy implications for users, and it is important users cannot be tracked by another person or application without the users affirmative express consent. We believe the consent should be timely and clear but industry needs to maintain flexibility in how to present the notice so companies should have ability to offer consent mechanisms in innovative and creative ways. We would urge the Commission to engage with key stakeholders from across the online and mobile ecosystems and from consumer, civil society and privacy organisations to discuss appropriate privacy default settings and how consent should be obtained, used and managed to ensure clarity, transparency and fairness to the person being located.

We would also suggest that any measures taken in respect of location privacy must consider the granularity of the data concerned. For example, is data that reveals the country or state from which a person is accessing Internet services 'sensitive', requiring affirmative express consent? What

about geographic location used from account records such as postal code? How are these location designations different? Some might consider such categories of location data are necessary for product and service fulfilment and so fall under the commonly accepted practices category. This lack of clarity and uncertainty in the Commissions report will not result in effective solutions.

We also would urge the Commission to engage in dialogue and co-operation with other agencies such as the Department of Commerce (DoC) and the Federal Communications Commission (FCC) to ensure a consistent approach and an effective overarching user-centric privacy framework that applies consistent rules to functionally equivalent data irrespective of business sector or technology. This is important considering the intentions of the DoC to support self-regulatory initiatives and codes of conduct[8]. It is important to have a level playing field in relation to the regulation of privacy and to ensure functionally equivalent data such as geolocation data is subject to a single set of rules that is neutral regards technology and business model. For example, mobile carriers are subject to additional rules in relation to ensuring the confidentiality and security of consumer proprietary network information (CPNI), where other online businesses that capture functionally the same information are not. This adds additional costs and resource burdens without enhancing the privacy of 'online' users but instead drives dual standards that do not provide consumers with consistent privacy experiences and protections. The converged and rapidly changing world of the internet, the web and mobile call for a rethink as 'online' internet players focus more on the transforming role mobile is playing across the world[9].

c. should the method of consent be different for different contexts.

As above we believe consent should not be the principle basis for collecting, using or sharing a consumer's personal information. The priority and key is to ensure consumers are made aware in clear and transparent ways how their data will be used, and in the mobile context are given simple device appropriate mechanisms for expressing choice and preference.

- *what are effective ways to seek informed consent in the mobile context given the multiple parties involved in data collection and the challenges presented by a small screen?*

  In the app scenario discussed above, it will be necessary to establish privacy design guidelines that assist in the development of technology solutions and that these guidelines are adopted on an industry wide basis. The guidelines should support innovation in privacy controls and ensure user confidence across technologies and devices.

  We support the development of 'privacy nudges' or prompts that are short, simple, instructive, contextually and device appropriate and non-intrusive on the consumer experience. The GSMA is investigating the development of nudges and prompts and we note the excellent work being

[8] Department of Commerce Internet Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (December 2010) http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf

[9] *Global CIO: Google's Eric Schmidt: Top 10 Reasons Mobile Is Always #1*, Information Week, **http://www.informationweek.com/news/global-cio/interviews/showArticle.jhtml;jsessionid=OFEIAB2ENBU2LQE1GHOSKH4ATMY32JVN?articleID=229100076&pgno=2&queryText=&isPrev=**

conducted by Professor Lorrie Faith-Cranor and colleagues at the CyLab Usable Privacy and Security Laboratory (CUPS) at Carnegie Mellon University[10]. We are also interested in other developments such as research being conducted by projects like the Privacy Rights Management for Mobile Applications (PRiMMA)[11] and research into 'Visceral Notice' by privacy expert Professor Ryan Calo[12].

We would suggest the Commission might progress this important issue by facilitating workshops between industry and other stakeholders with the objective of identifying and committing to pursue and deliver meaningful solutions.

- *would a uniform icon or graphic for presenting options be feasible and effective in this and other contexts?*

  The GSMA supports the development and use of consistent icons to compliment a layered privacy notice approach and the use of 'privacy nudges' to informing users of the privacy implications of applications and services. We note a number of initiatives looking at the viability of privacy icons and are concerned that too much diversity in this area may undermine the efficacy of icons and approaches.

  Current initiatives in this field include the Mozilla privacy icons project[13], the privacy 'pictograms' project of the independent research organisation TNO based in the Netherlands[14], the Cylab Cups team initiative[15], TRUSTe's mobile application privacy icon product[16] and research of independent designers[17] looking at the use of iconography in the mobile contactless payment space, or at exploring the use of icons for 'making privacy policies not suck'[18]. We are also aware of the good work being done by the cross-industry Self-Regulatory Program for Online Behavioral Advertising and the development of an 'advertising option icon'[19]. We would however, suggest this program demonstrates the need to consider the uniqueness of the 'mobile' and especially the touch-screen of the smartphone. It is unclear, for example, how the proposed advertising icon will work on a touchscreen smartphone when the icon has been developed for a PC mouse-driven user interaction. This is an important consideration given a recent survey that found that nearly half of mobile app users said they were more likely to accidentally click an ad than intentionally[20]. We would urge the commission to facilitate workshops with experts and cross industry players to investigate the development and use of effective icons that are relevant across the online ecosystem and business sectors, that are

[10] http://cups.cs.cmu.edu/
[11] http://www.open.ac.uk/blogs/primma/
[12] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1508893
[13] http://mozillalinks.org/wp/2010/12/privacy-icons-to-help-us-understand-web-privacy/
[14] http://www.slideshare.net/SaferInternetForum/privacy-pictograms-gabriela-bodea-tno-safer-internet-forum
[15] Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach
http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab09014.pdf
[16] http://www.truste.com/privacy_seals_and_services/enterprise_privacy/mobile_certification.html
[17] http://www.elasticspace.com/2005/11/graphic-language-for-touch
[18] http://www.azarask.in/blog/post/making-privacy-policies-not-suck/
[19] http://www.aboutads.info/participants/icon/
[20] 'App Users Click Ads by Mistake' http://www.ibtimes.com/articles/106449/20110128/advertising-smart-phones-mobile-apps.htm

culturally sensitive and effective across borders.

- *is there market research or academic studies focussing on the effectiveness of different choice mechanisms in different contexts?*

Please see various references above. The GSMA is currently preparing a research study into the privacy attitudes of mobile users. The research is intended to help support the design process, user interfaces, privacy nudges and prompts.

The GSMA believes the Commission and other agencies should bring academia, industry and NGOs together to pursue solutions. We are also of the view that the Commission should engage with other regulators and organisations in other international jurisdictions to ensure the effectiveness of the proposed framework.

A number of globally available and successful online services are provided to consumers around the world by businesses established in the US and that will be subject to the proposed regulatory regime. These services may be provided to more people outside of the USA than within the USA[21]. The privacy expectations of consumers in Europe, Africa, the Middle East, and Asia may be shaped by these global relationships and US-rooted privacy standards. It is important, therefore, that the proposed framework helps establish consistent privacy experiences to help establish confidence and trust for global consumers.

Practically, the FTC may provide guidance to consumers living outside of the US about their privacy expectations and rights when using the services of businesses established in the US but which businesses are not established in the country of the consumer. This consideration appears more urgent following the recent view of the European data protection authorities Article 29 Working Party (WP) and their '*Opinion 8/2010 on applicable law*[22]*'*. The Opinion appears relevant to the smartphone app market as it provides guidance and clarification on the scope and application of the EU Data Protection Directive[23] with regard to the processing of personal data within and outside the European Economic Area (the EEA). The Opinion states "*while providing geo-location service to individuals, the controller [located in New Zealand] will use the* ***mobile device*** *of the individual (through dedicated software installed in the device) as* ***equipment to provide actual information on the location of the device and of its user****. Both the collection of information with a view to provide the service, and the provision of the geo-location service itself, will have to comply with the provisions of the Directive."* This suggests a view that companies established the US but with no presence in Europe and who provide mobile applications via app stores to consumers in the EU and who utilise device and consumer data are subject to EU data privacy laws. It will be important to consumers that regulators address and clarify these issues.

[21] For example, approximately 70% of Facebook users are outside the United States. http://www.facebook.com/press/info.php?statistics
[22] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf
[23] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

d. *how should a universal choice mechanism be designed for consumers to control online advertising.*

Policy and industry approaches to enhancing a user's privacy options regards behavioural advertising are premised on fixed-line PC thinking and privacy by add-on. To date there appears to have been little focus on the degree to which solutions and approaches designed for the PC world can translate to the world of mobile smartphones. The sales and uptake of smartphones and rich web and app products continues to soar. With this comes an increasing interest in understanding browser and app behaviour for a range of legitimate business purposes by a diverse range of actors across the mobile ecosystem. A challenge is to develop simple, clear means and mechanisms that are context, device and OS appropriate and which provide users with meaningful ways to be aware of and to manage their privacy and express choice and preference over the use of their personal information.

The concept of 'do not track' is still being defined[24] and solutions currently being developed by Mozilla, Microsoft and Google. Each of the solutions will result in different user experiences and may require the ad industry and websites to adopt differing approaches. Mozilla has chosen a DNT HTTP header solution that will not be effective until websites begin to respect the consumer's request not to be tracked for behavioural advertising. Microsoft has chosen to use a list-based option. Google has opted to provide users of its Chrome browser with an add-on "*extension [providing] persistent opt-out of personalized advertising and related data tracking performed by companies adopting the industry privacy standards for online advertising*." A key issue relating to solutions dependent on the adoption of 'industry privacy standards for online advertising' is the question of which standards will apply and how consumers may understand those 'standards' and have confidence in them when the activities are global and consumers are established across the globe. For example, how will the new ad icon[25] work on a touch screen smartphone when the icon designed for the precision of a mouse or track pad actions.

e. *should the concept of a universal choice mechanism be extended beyond online behavioural advertising and include, for example, behavioural advertising for mobile applications?*

The GSMA believes that consumers should have the ability to express choice and preference regards the collection and profiling of their personal information for behavioural advertising irrespective of the technology or business model involved. We support the development of choice mechanisms for mobile applications, but believe that these mechanisms may reflect a specific business model.

For example, it may be legitimate for a provider of 'free' apps to not provide consumers with choice over the use of their behavioural data for advertising purposes. Advertising funds such free products and services. What is key is that the app should not access, collect or use consumer data

[24] "What Does 'Do Not Track' Mean? A Scoping Proposal by the Center for Democracy & Technology http://cdt.org/files/pdfs/CDT-DNT-Report.pdf

[25] http://www.aboutads.info/participants/icon/

for behavioural advertising or other secondary commercial purposes unless the consumer has been made aware in a clear and transparent manner of these intentions so the consumer can truly make an informed decision about using the app.

Gartner have predicted that Mobile apps will generate revenue of $15.9 billion in in 2012 and that this will in also drive hardware sales, advertising spending and technology innovation[26]. The wrong regulatory decisions or an overly prescriptive approach could seriously hamper innovation and economic growth in this key sector. We would urge the FTC to conduct further research on this matter and obtain expert views.

4. Companies should increase the transparency of their data practices – Improved privacy notices.

a*. what is the feasibility of standardizing the format and terminology for describing data practices across industries?*

The CYLab Cups team are conducting research into machine- readable policies for privacy. This approach would seem to go some way to offering a solution but further research needs to be done in the mobile sector, especially in respect of mobile OS.

The OECD is also conducting a review of the OECD privacy guidelines[27]. The OECD provides an online privacy generator[28]. The FTC may wish to consider engaging with the OECD on whether the privacy generator could be updated to reflect the dynamic and increasingly open nature of the online world and assist developers and others to produce privacy notices that contain minimum privacy elements that aid user comprehension and choice.

b. how can companies present these notices effectively on mobile or similar devices?

The GSMA is in the process of conducting research into this goal.

5. Promoting consumer privacy throughout their organisations and at every stage of the development of products and services

a. is there a way to prescribe a reasonable retention period.

We do not believe that retention periods should be prescribed except where deemed necessary by legislators as a result of due process. Privacy by design calls for companies to adopt a principle of data minimisation – collecting and holding only the minimum amount of data necessary to meet clearly identified and legitimate business needs and/or to meet legal obligations. This can be achieved by conducting privacy impact assessments and ensuring the collection and retention of data is proportionate, justified and lawful. Retaining data without a business need leads to waste and unnecessary costs to businesses – why retain data that has no purposes but which nonetheless

[26] http://www.gartner.com/it/page.jsp?id=1544815
[27] http://www.oecd.org/department/0,3355,en_2649_34255_1_1_1_1_1,00.html
[28] http://www.oecd.org/document/39/0,3746,en_2649_34255_28863271_1_1_1_1,00.html

attracts all the costs of compliance regards ensuring data are kept accurate and up to date and are kept secure and protected against loss, misuse, theft and so on.

6. Consumer Education

a. how can individual businesses, industry associations, consumer groups, and government do a better job of informing consumers about privacy?

Informing consumers about privacy first and foremost requires key stakeholders to engage in dialogue on the issues and the outcomes desired for consumers. Only then will it be possible to begin to establish education programmes that communicate consistently the key messages by the most effective means.

b. what role should governments and industry associations have in educating businesses.

The GSMA has extensive experience of working with governments, regulators and industry in establishing initiatives to educating stakeholders on a range of consumer protection matters. Please see http://www.gsmworld.com/our-work/public-policy/protecting_consumers.htm and our work on Children and Mobile Phones.

Associations can play a role in research and facilitating dialogue and agreement on key matters and on driving common approaches. Associations may also play a key role in establishing self—regulatory guidelines and codes.

The GSMA looks forward to engaging with the FTC on this important and pressing matter of consumer privacy.