



Europe

**GSMA Europe response to the European Commission
consultation on the framework for the fundamental right to the
protection of personal data**

22 December 2009

Martin Whitehead
Director GSMA Europe

Park View, 4th floor
Chaussée d'Etterbeek 180
1040 Brussels

E-mail: mwhitehead@gsm.org
www.gsmeurope.org

Register ID Number: 38516182135-93

About GSMA Europe

GSMA Europe is the European interest group of the GSM Association (GSMA), representing 171 members in 50 European countries/areas and serving 600 million customers. The GSMA is the global trade association representing more than 700 GSM mobile phone operators across 218 countries and territories of the world. In addition, more than 200 manufacturers and suppliers support the Association's initiatives as key partners. For more information, visit www.gsmeurope.org.

Introduction

GSMA Europe welcomes the opportunity to contribute to the public consultation on the EU legal framework for the fundamental right to protection of personal data. GSMA Europe supports the underlying data privacy principles established by the Data Protection Directive 95/46/EC and the e-Privacy Directive 2002/58/EC. These data privacy Directives have been significant in advancing notions of privacy and have to date helped foster core privacy standards and good business practice across Member States. However, technological developments and the increasingly global, interconnected and interdependent nature of online services calls for a more effective and flexible legal framework which recognises the technological and business realities shaping consumer experience today, and in order that industry can continue to deliver significant benefits to the information society around the world. This position is supported by Communication COM(2007)228, in which the European Commission acknowledges that “the intensive and sustained development of information and communication technologies (ICT) is constantly offering new services which improve people’s life” and that the current legal framework “may prove insufficient when personal data is disseminated worldwide through ICT networks and the processing of data crosses several jurisdictions, often outside the EU”¹.

Recognising the above, it is important that a legal framework establishes consistent standards and expectations, that it offers meaningful protection for personal data and privacy, and that it liberates individuals to engage with new services with confidence and trust, wherever and whenever a person engages with those services. It is increasingly the case that privacy expectations of consumers are becoming transboundary as they engage with global services. These expectations increasingly transcend the geographic boundaries of national law just as an individual’s data and use of global services flows across those same boundaries. Confidence, trust and appropriate and effective privacy protection must stretch across these boundaries.

In this regard, we believe it is also important that the consultation considers recital 2 of the Directive 95/46/EC, which states that “data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals”. It is important that the Commission ensures the legal framework serves these interests of individuals and businesses by ensuring simplified and more meaningful regulation based on the risk of real harm, as opposed to a perception of harm, and that regulation may apply “whatever the residence” of individuals and in support of economic and social progress.

Our response addresses the Commission’s specific request for views on:

- the new challenges for personal data protection, in particular in the light of new technologies and globalisation;
- whether the current legal framework meets these challenges;
- what future action would be needed to address the identified challenges.

¹ http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0228en01.pdf

The challenges for personal data protection in the light of new technologies and globalisation

The “always-on”, internet-enabled, location-aware, multi-tasking mobile device, together with new (and increasingly global) business models, services and practices, has increased the complexity of, and given rise to, new privacy and security issues facing users and the mobile industry today. The ability to access and transmit in real-time detailed personal and private information about a mobile user and their use of mobile services has grown phenomenally. A key challenge is to reinforce confidence and trust, by ensuring user privacy is respected and the security of user data is protected in accordance with new business models and dynamics, legal and regulatory developments and changing user expectations.

GSMA Europe members have worked hard to earn the confidence and trust of their customers, given the personal nature of the mobile phone and the direct relationships enjoyed with their customers. However, the changing dynamics and increasingly open and global nature of the mobile services model and value chain has led to many more external parties seeking access to and interest in a mobile user’s personal and private data to serve their business models. Such parties include web industries, device manufacturers, O/S vendors, application developers and providers, advertisers, and social media service providers who are able to access and otherwise use a mobile user’s personal and private data wholly independent of a mobile network operator. It is the case that mobile network operators no longer have the ability to effectively protect the privacy and security of their customers’ data as they once did. GSMA Europe members believe that transparent and consistent data privacy standards and obligations should apply to responsible parties that process the personal and private data of mobile users, irrespective of a business’ infrastructure and services.

With this complex new world in mind, we have identified a number of key challenges with the current legal framework and which relate to the interpretation and practical application of the Directives, and the disproportionate regulatory compliance burden which they place on legitimate business activities that pose no real harm to individuals or society. It is the view of GSMA Europe that focus should be placed on addressing real harm to the protection of an individual’s privacy.

The key challenges are:

1. Applicable law:

Globalised services and the international flow of data across electronic borders create uncertainties and difficulties in determining which specific geographically bound law applies in particular circumstances. This difficulty is compounded when the capture and subsequent processing of data takes place by organisations established in a territory outside of the EU, and whose global services are accessible to and used by EU based citizens.

Article 4 of the Directive 95/46/EC adopts the concept of “establishment” of a data controller or “equipment” in determining the applicability of its data privacy principles. In its Opinion 1/2008, the Article 29 Working Party argued that “a search engine provider that processes personal data, such as logs with personally identifiable search histories, is considered to be the controller of these personal data, regardless of the question about jurisdiction”². In considering the use of cookies, the Working Party further asserts that a “user’s PC can be viewed as equipment in the sense of Article 4(1)c of Directive 95/46/EC [as] it is located on the territory of a Member State [and that] the Working Party is therefore of the opinion that

² http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf

the national law of the Member State where this user's personal computer is located applies"³. Such views and opinions are based on old world fixed-line PC concepts, which are increasingly outmoded and of limited use in an interconnected mobile world, where global services are instantly available on demand, wherever an individual may be. This is especially the case with regard to an EU based mobile customer who may roam across EU member territories using an always connected internet enabled smartphone. As this customer roams and accesses the internet services provided by a global organisation outside of the EU, one must ask which law should apply. The issue becomes more complex as an EU citizen roams to a country outside of the EU and uses the internet services of a global organisation based in another non-EU third country- which law applies?

An example of the complexity and difficulty of applying old world concepts to the global digital economy, it is important to consider the following scenario. An EU based consumer may purchase a mobile phone from a mobile network operator established in the EU. Independent of that operator, the consumer may download a mobile application from a third party's web-based "application store". The application store may be established in the USA and provide access to applications supplied by independent application developers who may themselves be established in another non-EU third country. The application developer may independent of the application store provider enter into a contractual relationship with another third party mobile media analytics company to insert code into the application. That "code" may be designed to access information relating to the mobile handset and the consumer's use of the application and other applications. That information may be shared with the application developer and third parties based in yet other non-EU third countries, for purposes such as mobile media analytics, advertising or other purposes. The "information" may include a phone's unique identifier, the longitude and latitude of the device at the start and during the use of the application (whether or not the application is a location based service), together with other information about the use of the application, and the birth month, year and gender for certain social network applications that may be installed on the device, whether or not the processing of such data is necessary to the provision and operation of the application. Determining applicable law and compliance responsibilities and ensuring consumer rights are respected and protected in such scenarios is a challenge that is not helped by legal frameworks which do not account for developments in technology, business models and relationships and adoption by consumers of new services. For example, under the current legal framework, it would appear that Directive 2002/58/EC would not apply to the non-EU established third party web-based application store or the application providers or mobile media analytics companies who may process location and traffic data of mobile users, by virtue that they are not considered providers of publicly available electronic services. In these instances, the legal framework disproportionately and unfairly imposes burdens on mobile network operators by historic and outdated concepts of applying regulation to infrastructure as opposed to the processing of data irrespective of technology, infrastructure and business model.

Protecting the interests of individuals regardless of where and how data processing occurs should be a primary objective rather than the development and application of rigid geographically bound laws that are at odds with the commercial and cultural realities of the global information society and the needs of citizens. What is required is a legal framework that can be applied across borders, which is based on the concept of accountability and harm, and which draws on technological controls and self regulatory codes and mechanisms as supported by Articles 17 and 27 of the Directive 95/46/EC. "Accountability" is based less on prescriptive legislation and regulation and more on the adoption, commitment to and practice of core internationally recognised privacy principles and information governance standards. The "accountability" model is based on organisational assessment of risk and potential harm that may be caused to individuals, and the reliance of organisations to

³http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_en.pdf

establish information management systems and appropriate technological solutions to adequately address risks and protect the privacy of individuals. It is also dependent on individuals having effective recourse to organisations and regulators to address privacy failures. Such models have been considered in the RAND report on the review of the European Data Protection Directive commissioned the UK Information Commissioner's Office⁴.

2. Inconsistent and disproportionate bureaucratic interpretation and application of law

Member States have implemented the data privacy Directives in divergent and contradictory ways. Data protection authorities likewise have interpreted and applied applicable data privacy law in different and often conflicting ways. While a core objective of the data privacy Directives has been to harmonise data privacy protections and frameworks across the community, it appears to have had the opposite effect in practice.

Data protection and privacy compliance has become ambiguous, complex and increasingly bureaucratic as a result of the different interpretations and implementations of the data privacy Directives across the EU. Organisations now require significant expert legal guidance and resource across multiple jurisdictions in efforts to strive for compliance, which is burdensome, time consuming and costly, and which may not deliver required levels of awareness and understanding by consumers and those employed to protect them. Organisational resources should be freed to deliver meaningful and realistic protection of privacy based on identified risk.

One key area of disproportionate bureaucracy is the compliance requirement to notify data protection authorities of processing activities. In some Member States this requires simple notification of core processing activities, while in others processing is prohibited unless prior notification has been made and authorisation received, and detailed information supplied as to categories of data, disclosures, systems and security measures adopted. For multinational companies that operate in multiple Member States, this requires engagement with each data protection authority and navigation of each Member State's data privacy laws while delivering little if any real benefit to companies or their customers, as the situation within groups of companies is not properly recognised within the current Directive. This bureaucratic requirement diverts limited financial and organisational resource from companies and data protection authorities – resources that could be better utilised in fostering greater awareness and understanding of privacy. Recognising these issues, the recently formed European Privacy Association has established a working group to explore the: "Harmonisation of notifications to DPAs: reducing complexity for individuals and business"⁵.

Evidence suggests that "notification" registers maintained by data protection authorities are rarely consulted by the public and do not bring any additional benefits to consumers over and above the requirements of organisations to notify individuals of their processing activities. GSMA Europe believes that a more flexible system is required and which is based on the principle of accountability – that organisations should be free to meet their obligations to notify individuals of the identity of the organisation and its data processing activities. An organisation's privacy statement is often the first and most appropriate and meaningful notice that an individual will consult. Organisations should be held accountable by data protection authorities to meet the notification obligation by effective privacy notices made available or otherwise presented to individuals. A recent court of appeal case in the UK

⁴http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf

⁵http://www.europeanprivacyassociation.eu/2009/agenda_news.asp?funzione=scheda&id=16

highlights the weakness of formal notification, the issues with national implementation and suggests that organisational notice should take precedence⁶.

The concept of “accountability” has attracted increasing support from industry, privacy experts and privacy commissioners⁷, culminating in the 31st International Data Protection and Privacy Commissioners’ conference adopting a resolution on international data privacy standards, which included the principle of “accountability”⁸. It should be noted that the concept of “accountability” already exists in Directive 95/46/EC by virtue of obligations placed on organisations to determine the purposes of processing, whether data are adequate for specific purposes, to assess how much data to process, and what security measures are appropriate in all the given circumstances. The adoption of “binding corporate rules” (BCR) as a mechanism to ensure personal data are transferred globally in a trusted and protected manner is another example of the use of “accountability” by EU policy makers.

An effective data privacy legal framework should look to encompass the principle of “accountability” and establish recognised core elements to ensure such an approach is effective and responsive to regulatory and technology developments, and to consumer expectations and any reasonably identifiable harms. An effective accountability framework will require high degrees of transparency and openness on the part of organisations, the adoption and implementation of clear policies and procedures, training and education programmes, complaints handling processes, audit mechanisms and review and enforcement processes to identify and address any harms arising from data privacy practices. It will also require data protection authorities to be given the power to conduct inspections to ensure organisations are meeting their commitments to accountability.

Consideration could also be given the adoption of trustmarks or seals to strengthen the accountability of organisations. Trustmarks can deliver independent verification of an organisation’s practices providing assurance to regulators and consumers alike. Indeed, a 2007 EU report, “Comparison of Privacy and Trust Policies in the Area of Electronic Communication”⁹ advised that “trustmarks are a relatively unintrusive approach that can serve as a useful complement” to legal and regulatory privacy protection frameworks. The report recognises that “the privacy label approach is not much used in Europe, but [that there is] no reason in principle why the use of trustmarks could not be expanded [in the EU and that the] topic merits further study”.

3. Lack of clarity in the Directives and ambiguity concerning legal concepts and definitions

The data privacy Directives contain legal concepts and definitions that do not lend themselves to consistent, meaningful interpretation and application by data protection authorities or global businesses. There exists an urgent need to clarify existing data protection concepts and definitions such as “personal data”, “data controller”, “data processor” and “consent”, particularly in light of technological developments, such as cloud computing, which do not fit clearly into one definition or another. These remain subject to significant deviations in interpretation by Member States and increasingly appear out of date

⁶ <http://amberhawk.typepad.com/amberhawk/2009/11/could-notification-to-the-commissioner-undermine-three-data-protection-principles.html>

⁷ See the paper “Data Protection Accountability: The Essential Elements A Document for Discussion” (October 2009) produced by the Galway Project, available at http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf

⁸ http://www.privacyconference2009.org/privacyconf2009/dpas_space/space_reserved/documentos_adoptados/common/2009_MADRID/estandares_resolucion_madrid_en.pdf?privsession=83cda07caf1e870c7b4b33c32b4ac1b9

⁹ http://ec.europa.eu/information_society/policy/ecomms/doc/library/ext_studies/privacy_trust_policies/final_report_29_02_08.pdf

in a globally interconnected world of “digital citizens” that is based on data passing electronically across international borders.

Personal Data:

Article 2 of the Directive 95/46/EC defines personal data in very broad terms as “any information relating to an identified or identifiable natural person” and that an “identifiable person is one who can be identified directly or indirectly...by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”. The Article 29 Working Party also issued an opinion¹⁰ on personal data and stated that “information” “relates” to a person where it may have a direct impact on the person. This has led some Member States to apply the definition of “personal data” to location data, to an anonymous web profile, or to an IP address on the basis that an “individual is 'identified' if you have distinguished that individual from other members of a group”¹¹ even though an organisation collecting and processing such information has no intention of using it to target or in any way affect a specific individual.

Recital 26 of the Directive 95/46/EC qualifies whether or not the individual is identifiable, by stating that it depends on “all the means likely reasonably to be used either by the controller or by any other person to identify the said person”. In many cases it seems that data protection authorities have not uniformly interpreted this qualifying principle, and have chosen instead to adopt a broad approach. This can lead to the excessive and burdensome imposition and adoption of technologies and processes to render such data wholly “unidentifiable” in the eyes of data protection authorities when a more purposive approach should be taken, in which context should determine the degree to which a piece of “data” is personal data. For example, in the hands of an internet service provider, it may be possible to identify an account holder for an IP address but not an individual using a computer linked to that address. That same IP address may necessarily be collected by a website operator in order to meet a request from the user of a PC or mobile device. Do these examples amount to personal data being processed? This question becomes more difficult to answer when we consider that an IP address may be dynamically assigned - changing with each log-on of the computer or access to the internet - or when we consider that mobile network operators may assign a single gateway IP address simultaneously to many thousands of customers (who may use anonymous pre-paid services). An example of the uncertainty over such issues can be found in a consultation for an “Online Personal Information Code of Practice” recently launched by the UK Information Commissioner’s office¹². The code is inconclusive on whether IP related data is personal data, and advises that the Information Commissioner “recognises the practical difficulties, sometimes insurmountable ones, in complying with all aspects of the [law] in respect of non-obvious personal identifiers”. The code goes on to state that “most organisations operating online will never be able to ascertain whether a particular device has a single user or a number of users. [but that], this does not mean that personal data is not being processed by them”. Such views and interpretations do not deliver the necessary clarity required to ensure consistent and effective privacy practices that enable organisations to pursue their legitimate interests and use data to shape the future of their services and deliver benefits to their customers, where such use poses no harm to customers. Continued ambiguity can only serve to foster anxiety and fear among consumers, prevent their engagement with services and restrict business investment in and development of new information society services.

¹⁰ Opinion 4/2007 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

¹¹ UK Information Commissioner’s Office, “Technical Guidance to Determining What is Personal Data” http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_data_flowchart_v1_with_preface001.pdf

¹² <http://ico-consult.limehouse.co.uk/portal>

Data protection authorities have also taken inconsistent approaches to the anonymisation of data caught by both data privacy Directives. In some cases they require organisations to obtain the consent of individuals or as a minimum to provide an opt-out, even though there is no intention to identify or target specific individuals, but rather to use data for the legitimate purposes of statistical analysis and measurement to identify services used and plan and develop future services. Such positions seem counter to the Opinion 4/2007 of the Article 29 Working Party, which found that “anonymous data in the sense of the Directive 95/46/EC can be defined as any information relating to a natural person where the person cannot be identified, whether by the data controller or by any other person, taking account of all the means likely reasonably to be used either by the controller or by any other person to identify that individual”. The Opinion further states that “anonymised data” would be anonymous data that previously referred to an identifiable person, but where that identification is no longer possible, and quotes Recital 26 of the Directive 95/46/EC as supporting this position, in that it states that “the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable”.

The current legal framework is overly dependent on whether or not data can be defined as “personal data” without ever coming to a realistic interpretation that is fit for purpose in the digital economy. Overly restrictive interpretations of the definition of personal data are creating unnecessary barriers and impediments to the legitimate activities of organisations where such activities pose no risk to the privacy of individuals and where such activities are crucial to developing and delivering information society services that are increasingly crucial to economic growth.

As introduced above, there is an additional effect of the existing data protection regimes that is particularly damaging to the mobile industry. The e-Privacy Directive imposes additional obligations only on electronic communications service providers for certain kinds of information thought to be particularly sensitive. But information about consumers’ activities online – which would in the hands of the mobile industry be protected as traffic data - and about their geographical location – otherwise, location data - can, in today’s globally interconnected world, be obtained from many other sources. As a concrete example, location data obtained from a mobile network operator’s GSM or 3G networks is regulated by the e-Privacy Directive and subject to the consent of individuals where processing of such data is required to deliver a value added location based service. However, precise location data such as GPS data indicating the longitude and latitude of a mobile device, may be accessed and used wholly independent of a mobile network operator, by companies who provide applications that do not appear to be regulated by the e-Privacy Directive. This regime does not adequately protect the data privacy interests of mobile users and places discrepant burdens on the use of functionally equivalent data based solely on the industry the data controller finds itself in. Mobile operators’ hands are tied with respect to traffic and location data, making it difficult to compete with new players in the field who are not subject to such restrictions, and with no greater protection to consumer privacy.

What future action would be needed to address the identified challenges?

It is important that policy makers and regulators avoid excessive bureaucracy and using data privacy law to prevent rather than facilitate activities that bring benefits to society where there is no possibility of harm to individuals. It is time to consider a more risk-based approach to the protection of personal data and privacy, which first and foremost considers the harm or potential for harm that processing might pose to individuals or society. A more pragmatic interpretation of concepts and greater harmonisation is required within the context of an interconnected global citizenry.

We agree with the conclusions of the recent report of the advisory board of RISEPTIS, that “Policy makers and regulators will be most effective if they base their work on sufficient

technological insight and the expectations of business, consumers and public organisations”. We support a 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. For example, such fora could help establish self regulatory standards that are flexible and responsive to technological developments and which compliment applicable law.

We would urge the Commission to:

- Consider the need for simplified notification procedures that can apply across all Member States, or indeed, consider whether notification serves any real purpose. Consideration should be given to reliance on organisations providing individuals with adequate and compliant privacy notices under the accountability principle.
- Review the concept of personal data and ensure a harmonised interpretation and application across all Member States, and which can apply to services of a global nature. We would also urge the Commission to adopt a process oriented layered approach to ensure any definition is dependent on context, so as not to capture categories of data from which it may be impossible to identify an individual or which presents no harm to individuals.
- Consider the mutual recognition of decisions by national data protection authorities on the basis of the “country of origin” principle.
- Review the principles on applicable law. It is apparent that the current rules are excessively bureaucratic, impose undue burdens on organisations, restrict innovation and may work to erect barriers to start-ups or those who are unable to employ the significant legal expertise and organisational resource currently needed to navigate and comply with the “applicable rules”. It is vital that a simplified framework is developed which is intelligible to individuals and businesses and which affords real and meaningful protection and regulatory recourse.
- We would ask the Commission to consider removing barriers to competition that arise because functionally equivalent data, made widely available through developments in technology (e.g. GPS location data) are treated disparately under the existing legal framework.
- Consider the creation of a privacy trustmark that is effective, proportionate, affordable, and globally applicable and which fosters meaningful levels of confidence and trust among regulators and consumers and by which organisations can be seen to be “accountable”.

In closing, we should like to draw the Commission’s attention to the RAND report and its acknowledgement that “personal data helps companies efficiency gains (extracting more commercial value or profit from existing customers via better tailoring of products and services to the market) or enabling cost cutting in the private and/or public sector by eliminating inefficiencies but also innovation (providing new products and services based on understanding customers through the interrogation/re-use of their personal data)”. We would urge the Commission to consider the significant benefits brought by the mobile industry and to achieve an appropriate, effective and workable balanced framework that is industry, sector and technology agnostic, to take the new mobile ecosystem circumstances into account, and create a consistent experience for mobile users where all entities dealing with their data are subject to the same rules, regardless of their establishment or the nature of the product or service offered.

We also consider that to be successful in establishing an effective and balanced legal framework, it will be necessary to meet the obligations of and expectations set by the Lisbon Treaty which brings the Charter of Fundamental Rights into European primary law. The Charter states that “Everyone has the right to the protection of personal data concerning him or her” and that “such data must be processed fairly for specified purposes and on the basis

of the consent of the person concerned or some other legitimate basis laid down by law". One of the challenges faced is ensuring proper interpretation and setting realistic expectations of this newly enshrined human right and avoiding the ambiguous over bureaucratic interpretations and applications experienced to date.