TRANSATLANTIC CONSUMER DIALOGUE (TACD)
2005 RECOMMENDATIONS REPORT

AND

EUROPEAN COMMISSION SERVICES' RESPONSES

June 2006

TACD

TRANS ATLANTIC CONSUMER DIALOGUE

DIALOGUE TRANSATLANTIQUE DES CONSOMMATEURS

TACD 2005 RECOMMENDATIONS REPORT

As part of its role as a consultative forum to the EU and US, TACD makes policy recommendations on issues of concerns to its European and American members.

This report brings together the recommendations made in 2005, to allow the governments to formally respond. It is the second of an annual collection TACD's recommendations in a year-end report to governments and the public.

TACD represents the demand side of the two biggest economic blocks in the world - the 735 million U.S. and EU consumers. Its network of 65 EU and U.S. national consumer organisations has a direct paid-up membership of some 20 million consumers.

On both sides of the Atlantic, these groups have long track records of achievement in the consumer protection and safety fields. Many have successful publishing, research and product testing operations as well as advocacy and policy activities and are self-financed; others, according to their cultural traditions, are financed from public or foundation funds. All are independent.

More information can be found at www.tacd.org .

INDEX

The 2005 Recommendations Report covers TACD recommendations on

Trans-Fatty Acids

March 2005, Food-25-05

(this is limited to the recommendations – for the full resolution with background and research findings, go to www.tacd.org/docs/?id=277)

There is now strong evidence that consumption of trans fatty acids increases the risk of cardiovascular disease. Trans fatty acids offer no nutritional benefit and, given the health concerns, there is no reason why food producers should continue to include fats containing trans fatty acids within their products.

TACD therefore:

- urges the European Union and the United States governments to establish specific targets for food producers to eliminate artificially produced trans fatty acids from their products

- urges the European Commission to address the issue of labeling of trans fatty acids as part of its planned review of the nutrition labeling directive.

***

European Commission Services' Response

The Commission is aware of the evidence on the impact of trans fatty acids on health and there is an opinion of the European Food Safety Authority's[1] on this subject. Trans fatty acids can be formed during the processing of fats and oils, including hydrogenation. In addition, trans fatty acids can be naturally present in foods of animal origin, such as dairy products and meat from certain animals The scientific evidence indicates that higher intake of trans fatty acids is associated with a potential increased risk in coronary heart disease and that other dietary factors, for example intake of saturated fatty acids, can also have an impact.

The Commission is committed to using the appropriate means that are available to it to promote consumer protection and health. One area of activity in relation to nutrition is the European Platform for Action on Diet, Physical Activity and Health[2]. Voluntary reformulation of products is part of a number of commitments from the food industry and members of the Platform have put in place initiatives aimed at reducing the amount of fat, in particular saturated fatty acids and trans fatty acids, in their products. The extent of these actions on reformulation should become apparent as the work of the Platform progresses, particularly in relation to monitoring of commitments. Such initiatives would be expected to have a positive impact on the potential risk factors for cardiovascular disease.

Information about the content of foods, be this via ingredient listing or nutrition labelling, is an important element in empowering consumers to make informed choices about their diet. Especially when used with relevant consumer education. It is anticipated that during the discussions on the revision of the nutrition labelling directive, the need to include trans fatty acids as part of the nutrition labelling information will be discussed. Along with, as necessary,

[1] Opinion of the Scientific Panel on Dietetic Products, Nutrition and Allergies on a request from the Commission related to the presence of trans fatty acids in foods and the effect on human health of the consumption of trans fatty acids. (see http://www.efsa.eu.int/science/nda/nda_opinions/588_en.html).

[2] See: http://ec.europa.eu/health/ph_determinants/life_style/nutrition/platform/platform_en.htm

consideration of the appropriate definition of trans fatty acids for labelling purposes, taking into consideration international discussions on this issue.

The responses to the recent public consultation on the Commission's Green Paper *"Promoting healthy diets and physical activity: a European dimension for the prevention of overweight, obesity and chronic diseases"* [3] will be taken into consideration in any future Commission action on trans fatty acids. As will the responses to the consultative document on "*Labelling: Competitiveness, Consumer Information and Better Regulation for the EU*"[4].

[3] http://ec.europa.eu/comm/health/ph_determinants/life_style/nutrition/documents/nutrition_gp_en.pdf

[4] http://ec.europa.eu/comm/food/food/labellingnutrition/betterregulation/index_en.htm

Radio Frequency Identification (RFID)

March 2005, Internet-31-05

(this is limited to the recommendations – for the full resolution, including a detailed description of the risks for consumers, go to www.tacd.org/docs/?id=274)

TACD resolves that the EU and US governments should:

1. Analyze whether existing data protection and privacy regulations adequately address the privacy risks that the applications of RFID present for consumers in different contexts and sectors; determine the appropriate safeguards; and enact the legislation and regulations necessary to eliminate those risks.

2. Ensure that the implementation of RFID technology complies with existing data protection and privacy legislation (such as the Data Protection Directive and the Directive on Privacy and Electronic Communications in the EU) and privacy guidelines (such as the OECD's principles of fair information practice). For example, RFID must be used transparently, so that consumers know (and can choose) when RFID is being used; and know who is collecting the data and why. Consumers must also be given the right to access their information. In particular, the EU and US governments should require organisations developing and using RFID to follow the following principles (the first four (a – d) are set out in the International Conference of Data Protection & Privacy Commissioners "Resolution on Radio Frequency Identification Technology", 2003):

   a. Before introducing RFID tags linked to personal information or which help build consumer profiles, organisations should first consider alternatives that achieve the same goal without collecting personal information or profiling consumers;

   b. If organisations can show that personal data are indispensable, they must be collected in an open and transparent way;

   c. Personal data should only be used for the specific purpose for which they were first collected and only retained for as long as is necessary to achieve that purpose;

   d. Whenever consumers possess RFID tags, they should be given the option of deleting data and disabling the tags;

   e. Any ID-based RFID should be designed to be accessible only with the consent of the person.

3. Finally, at retail-level there should always be the possibility to pay anonymously without using payment-cards, store cards or any other personal data payment system.

4. Vigorously enforce laws and regulations that apply to RFID.

5. Monitor whether RFID is being used in anti-competitive ways, and use anti-competition laws to prevent such abuse.

6. Consult with all RFID stakeholders, including consumer organizations and independent academic researchers, to tap into the range of expertise that could usefully contribute to this debate.

7. Fund ongoing research into the impact of RFID on consumers, particularly those who are disadvantaged (such as those who are disabled and on low incomes), and their perceptions of the technology. Research must be undertaken in a transparent, independent, and scientific way.

8. Require organisations that use RFID to automatically de-activate the tag after the consumer has purchased the product, giving the consumer the option of re-activating the tag where that might be appropriate.

9. Commission independent and scientific research to investigate the safety of RFID and its environmental impact.

Furthermore, TACD resolves that organisations developing and using RFID should:

1. Provide evidence of real consumer benefits from the use of RFID and address its potential risks. If organisations make claims that specific consumer benefits will accrue from using RFID, these promised benefits must be delivered.

2. Build security and privacy protection into the technology and its applications. This would include ensuring that sensitive data are encrypted and that data confidentiality and integrity is maintained (so that, for example, information is protected from unauthorised third-party access). Protection must not be seen as an optional extra but as an integral part of deploying this technology.

3. Explore positive uses of the technology that enhance consumer privacy and decision-making. For example, scanners could alert consumers to opportunities to make choices, access information on products, and offer real-time access to their data.

4. Explore the potential of RFID to extend consumer choice and reject applications that have potentially anti-competitive effects.

***

European Commission Services' Response

RFID potentially represents considerable opportunities for economic growth in our modern economies. At the same time, RFID technology intertwined with sophisticated databases and networks might allow easily the collecting, storing, distributing and combining of digital trails of our daily transactions.

In this respect, the Commission has launched a wide public debate including a series of workshops. One of them has specifically addressed privacy, security and safety aspects of RFID. These workshops will assist the European Commission in drafting a working document on RFID. This document will be published in September 2006 in an online consultation. Additional feedback obtained will then be analysed and integrated in a Commission Communication on RFID, to be adopted before the end of the year 2006. This feedback will also contribute to the debate on the review of the e-privacy-Directive this year. The Communication will also address the need for other legislative measures for RFID.

In the meantime, the Article 29 Data Protection Working Party[5] has elaborated a Working Document (WP 105[6]), which provides guidelines to RFID deployers on the application of the basic principles set out in the EC directives and guidance to manufacturers of RFID technology towards designing privacy compliant technology in order to enable deployers of the technology to carry out their obligations under the data protection directive. The public consultation that followed the adoption of this Working Document has generated a huge interest from stakeholders.

Furthermore, the Article 29 Data Protection Working Party has set up a subgroup on RFID with the main goal to analyze the concept of personal data, analyze how far RFIDs are covered by the Data protection directive, and find out whether data protection interests are adequately covered by the existing law, and if necessary, make proposals on legal amendments to the Data protection directive or for other measures.

Personal data are not involved and processed in all RFID operations. However, insofar as personal data are involved in RFID operations, data protection legislation and privacy principles must apply. e.g.: data quality, legitimate grounds for processing, information requirements, right of access, security, etc. How these principles translate for each type of application will depend on these applications.

So far several specific data protection concerns have been identified regarding RFID deployment The first type of risks arises when the deployment of RFID technology is used to collect information that is directly or indirectly linked to personal data. A second type of privacy implication arises where personal data is stored in RFID tags. A third type of data protection implication arises from uses of RFID technology which entail individual tracking and obtaining access to personal data.

Technology will play a key role in ensuring compliance with the data protection principles in the context of processing personal data collected through RFID technology. If deployers of an RFID application are ultimately responsible for the personal data gathered through the application in question, manufacturers of RFID technology and standardization bodies must ensure that privacy compliant RFID technology is available to ensure that data controllers through RFID technology have the necessary tools to implement the requirements contained in the data protection directive.

Finally, the European Commission is also planning to support, in the forthcoming Seventh Framework Programme (FP7) on Research and Technological Development, and in the Competitiveness and Innovation framework Programme (CIP), projects that will explore the policy implications of innovations in this area, and more specifically the perspective of consumers, of those who are disabled or have a low income, in line with the Commission objective to assure an inclusive eSociety.

[5] The Working Party established by Article 29 of Directive 95/46/EC is an independent EU Advisory Body of Member States Representatives on Data Protection and Privacy http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

[6] http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf

Digital Rights Management

April 2005, IP-01-05

(this is limited to the recommendations – for the full resolution, including a detailed description of the risks for consumers, go to www.tacd.org/docs/?id=275)

TACD urges the governments of the United States and the European Union to set certain preconditions that DRMs have to meet in order to qualify for legal protection. The preconditions recommended by TACD are set out below:

Access to and use of content
DRM systems that are capable of being used in excess of what is necessary to protect copyright will not receive the privilege of anti-circumvention protection.

DRM systems that define social entities such as 'household' and 'families' in their technology, and that define these entities more narrowly or restrictively than have been defined in local law or custom will not receive the privilege of anti-circumvention protection.

DRM systems that block the use of assistive technologies employed by disabled people will not receive the privilege of anti-circumvention protection.

Privacy
DRMs should be certified as compliant with data protection rules or privacy rights by the Data Protection Registrar or privacy enforcement agency before they are introduced onto the market. By building privacy interests into the design of the DRM, privacy rights may be enforced more effectively.

In particular, DRM systems should not use registration, use data, or other personal information for secondary purposes without first obtaining the individuals' informed and voluntary consent. That is, the individual should be able to use the media without consenting to marketing or other secondary uses of their personal information.

Interoperability
DRMs that restrict the normal expected usage of that product, such as space and time shifting, should not receive the privilege of anti-circumvention protection.

DRMs whose licensing and implementation terms preclude the use of Free and Open Source Software (FOSS) will not receive the privilege of anti-circumvention protection.

Transparency
DRM systems that are 'updated' without a user's consent will not receive the privilege of anti-circumvention protection.

All equipment containing DRMs must be clearly labelled showing what uses are allowed and what equipment it will or will not work on. DRM systems that are marketed without adequate disclosure of restrictions will not receive the privilege of anti circumvention protection.

Security
DRM software should not hamper or limit the use of software protection software on consumer computers. DRMs should not bring new vulnerabilities into consumers computing equipment and such systems must not interfere with consumers' ability to set and retain their own polices and levels of security for their own machines.

Anti-competitive behaviour
The potential anti-competitive effects of DRMs should be reviewed. In particular, a competition investigation should be undertaken into the licensing terms for DRM technology and the effect on competitors and complementary producers.

Redress
Consumers must have clearly defined and enforceable consumer rights that cannot be overridden by contract terms, DRM systems or other technological measures. They should not have to rely, as now, on the restraint or goodwill of the rights holders or, as in Europe, on the whims of each Member State as to which consumer exemption they will allow.

Among the consumer rights that should be clearly expressed:
right to private copy
right to fair commercial practices
right to be informed and refunded for faulty products
right to privacy and data protection.
right to free speech

A simple and speedy alternative dispute resolution system should be established for cross border DRM disputes so consumers do not have to rely on costly litigation for low value disputes, whilst retaining the right to use court action as a last resort.

***

European Commission Services' Response

The Commission will continue to closely monitor the development of DRM technologies and of the emerging market of DRM protected content distribution, and assess its compliance with economical and social objectives set out in various EU policies (Information Society and Media, Internal Market, Competition, Consumer protection).

The Commission's main objectives concerning Digital Rights Management systems (DRMs) are:

- To ensure adequate protection of copyright protected content, which is a condition for the availability of 'rich' online content.
- To contribute towards the take-up of DRMs in order to achieve digital technologies' full potential in terms of creation, dissemination and access to 'rich' online content, therefore promoting the development of the information "space" and the content industries.
- To ensure a high level of consumer protection and make sure that DRM shall not be used to lower consumers' rights. This is, in itself, a condition for the take-up of the new services which are made possible by DRMs.

Furthermore, the Commission strongly supports open standards as the way forward for DRMs. However, they should be voluntary and market-driven. It is clear that interoperability is a key element. Therefore, the Commission will encourage the industry to take steps towards interoperability. The i2010 strategy[7] intends to address the issue of the interoperability of DRM systems.

DRM systems are addressed within the EU legal framework in Directive 2001/29/EC of 22 May 2001 on the harmonisation of copyright and related rights in the Information Society. Directive 2001/29 grants protection to technological measures and rights management information under Article 6 and Article 7, respectively. In doing so, this Directive implements the Community's obligations under the 1996 WIPO Treaties, namely the WIPO Copyright Treaty and the WIPO

[7] http://europa.eu.int/information_society/eeurope/i2010/index_en.htm

Performers and Phonograms Treaty. Directive 2001/29 sets out that protection is only given to technological measures which are designed to prevent or restrict acts, in respect of works or other subject matter, which are not authorised by the rightholder of any copyright or any right related to copyright or the sui generis right provided for in Directive 96/9.

However, the Community legislature considered it appropriate to set out a mechanism which ensures the availability of certain public interest exceptions where there is a technological measure in place. According to article 6(4)1 of Directive 2001/29, Member States are required to act in the absence of voluntary measures taken by rightholders, such as agreements between rightholders and other parties concerned, to ensure that the exceptions or limitations provided for in their national law are available. These exceptions include notably the reproduction on paper or any similar medium; specific acts of reproduction by certain publicly accessible libraries; ephemeral recordings or works made by broadcasting organisations; broadcasts made by certain social institutions; use for teaching or scientific research; use for the benefit of people with a disability; use for the purposes of public security.

However, as far as private copying is concerned, under article 6(4)2 of Directive 2001/29, in general terms, Member States may decide (but are not obliged) to ensure the availability of the private copying exception if the rightsholders themselves have not taken any action. In any case Member States' action cannot prevent rightsholders from adopting measures regarding the number of copies. For the time being, only a minority of Member States have introduced in their implementing legislation a mechanism to deal with the private copying exception.

More specifically, Article 6(4)4 of Directive 2001/29 deals with the interactive on demand environment, i.e. when consumers contract on a one to one basis, as opposed to those cases when they make use of an exception. In this case, Member States cannot ensure the availability of the private copying exception. Nevertheless, consumers in such instances may still avail themselves of unfair contract terms law, data protection legislation and other provisions designed to protect their rights.

In addition, article 12 of Directive 2001/29/EC foresaw a report on the application of this Directive which would take into account in particular "whether the obligations as to technological measures confers a sufficient level of protection and whether acts which are permitted by law are being adversely affected by the use of effective technological measures". The Commission will review the anti-circumvention protection and its impact on acts which are permitted by law in the context of this report scheduled by the end of the year.

In October 2004, the Commission consulted Member States and all relevant stakeholders in order to assess whether DRM systems (systems that enable digital solutions to license rights and administer payments of royalty individually) were being successfully deployed and consistent with the provisions of the 2001 Copyright Directive. The Commission asked Member States to provide details on whether DRMs were being successfully deployed in a manner which allowed levies to be “phased out” or reduced in favour of other forms of compensation which were more direct and less costly to administer. The consultation revealed that levies are unequally applied in terms of equipment, media and amounts across Member States and that there is a lack of transparency in relation to their collection and distribution. The availability and use of DRM technologies have not had an impact on Member States’ policy with respect to levies. The Commission's services are therefore conducting an impact study on levy systems within the EU, based on empirical evidence, with a view to drawing up a policy proposal by the end of 2006.

Finally, DRM deployers are required to comply with data protection and privacy laws. Therefore DRM systems should be designed in a way complying with given data protection and privacy principles (as provided in recital 57 of Directive 2001/29/EC, DRMs should incorporate privacy

safeguards). One of these principles is that data collected via DRM shall be used only for the purpose they have been collected. The EC legislation notably requires the data subject to express his/her prior and unambiguous consent, i.e. informed and freely given consent. However, existing data protection laws do not foresee a certification system as described by the TACD. One of the ways for better implementation of the Data protection directive is to promote privacy enhancing technologies.

The European Commission intends to call upon enforcement authorities to prevent software products such as DRM, being built in a way that impairs compliance with the data protection legislation.

Broadcasting Rights Treaty

April 2005, IP-02-05

(this is limited to the recommendations – for the full resolution, including a detailed description of the risks for consumers, go to www.tacd.org/docs/?id=276)

TACD urges the governments of the United States and the European Union:

- To justify why a broadcast treaty based on copyright, rather than a 'signals' based approach, is necessary.
- To refrain from exerting further pressure to finalise the provisions on exemptions and limitations until the intergovernmental meetings proposed by Brazil and Argentina to discuss whether there should be mandatory minimum exemptions has taken place.
- To support the removal of the technical protection and anti-circumvention provisions in the Proposed treaty
- To encourage WIPO to a) provide an assessment of whether existing TPMs have successfully protected IP rights and what their impact on innovation and the exercise of consumer access has been. b) undertake a comprehensive study on the likely impact of TPMs on the Development Agenda.
- For the US to withdraw its support for the inclusion of webcasting
- To refrain from further pressure to hold a Diplomatic Conference.

***

European Commission Services' Response

WIPO has been working on updating the intellectual property[8] rights of broadcasting organisations since 2001. The rights of other major rightsholders namely authors and holders of other related rights .i.e. record producers and performers were updated in 1996 with the adoption of the so called WIPO Internet Treaties namely the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. Broadcasting organisations are the only group whose rights, at international level, are still governed by a Treaty concluded in 1961. i.e. the Rome Convention of 1961 on the rights of broadcasting organisations. The Commission has consulted Member States on the nature and scope of a possible instrument and the likelihood of success of a Diplomatic Conference. Without exception, Member States have indicated that they are committed to the process within WIPO in the light of their commitments to the United Nations and the international multilateral treaty-making process. Otherwise, the risk is that the international multilateral process will be replaced by bilateral agreements which would not necessarily be of assistance to all Contracting Parties to WIPO, including those associated with the Development Agenda. To a certain extent, Member States are prepared to show flexibility in relation to the scope of an instrument in order to achieve an agreement. However, any such flexibility will have to be consistent with international norms in this area.

[8] Copyright and related rights are the relevant intellectual property rights. Authors i.e. creators hold copyright whereas other groups of rightholders are described in the relevant international conventions as being holders of related rights i.e. rights related to copyright. The related rightholders are record producers that hold rights in sound recordings; performers in their performances and broadcasting organisations in their broadcasts. The term of copyright is longer (70 years after death of the author) than the term of related rights (50 years after fixation).

The aim of these negotiations is to update the Rome Convention. The starting point is, of course, the fact that broadcasting organisations already enjoy protection as holders of "related rights". In other jurisdictions broadcasters hold "copyrights". Therefore, a treaty based only on signal protection would be a departure from the family of intellectual property treaties and it would be considered a treaty of a sui generis nature which may not sit happily with the legal traditions of the majority of Contracting Parties. In addition, this would not reflect the legal tradition of any of our Member States.

The current texts on the table abide by the established intellectual property treaties including the Berne Convention, as amended by the Paris Act 1971 and in particular the 1996 WCT[9] and WPPT[10] which updated copyright for the digital environment but which did not deal with the rights of broadcasting organisations. The 1996 WIPO Treaties introduced at international level, protection for TPM[11] for holders of copyright and related rights. Directive 2001/29 on the harmonization of copyright and related rights in the Information Society transposes these obligations at Community level but also includes broadcasting organisations within its scope. The current draft texts are consistent with the approach of the 1996 WIPO Treaties in extending protection of TPMs to broadcasting organisations.

To that end, the position of the European Community and its Member States is reflected in the treaty language proposal submitted to WIPO in 2001, as amended by a further submission in 2003. These submissions reflect the high level of protection that broadcasting organisations enjoy within the EU as holders of related rights. To that extent, the EU cannot agree with the TACD demands since it would not reflect the current level of protection that is already accorded to broadcasters in the Community copyright acquis and would have the effect of diluting that protection.

Nor would it be feasible within the context of international negotiations for a new treaty updating the rights of broadcasting organisations in the intellectual property context under the auspices of the World Intellectual Property Organisations to depart from the substantive norms of previous treaties. This is what the Brazilian and Argentinean proposals envisage, namely the provision of mandatory rights for users. This would be contrary to all previous relevant Treaties in this area. The traditional approach in this area and the one which reflects EU law as well is to introduce optional exceptions for certain users such as the disabled or for teaching and research purposes.

During the 14th Standing Committee on Copyright and Related Rights (SCCR) in May 2006 in Geneva, the European Communities and its Member States submitted a formal proposal further elaborating on its suggested approach with respect to "limitations and exceptions" to the proposed broadcasters' rights. These proposals were very well received by the SCCR and were especially useful in bridging some of the major gaps that existed between developing and developed countries. The SCCR agreed to hold another session of the SCCR prior to the WIPO General Assembly in September 2006 that dealt with traditional broadcasters' rights only.

9 WIPO Copyright Treaty
10 WIPO Performances and Phonograms Treaty
11 Technological Protection Measures

Mobile Commerce

August 2005, Infosoc-32-05

(this is limited to the recommendations – for the full resolution, including a detailed description of the risks for consumers, go to www.tacd.org/docs/?id=283)

TACD resolves that the EU and US governments should:

1. Assess whether existing laws and regulations apply to mobile commerce, identify gaps, and examine inconsistencies in laws and regulations among EU member countries and between Europe and the US;
2. Solicit public input about appropriate consumer protections for mobile commerce via formal rulemaking proceedings, consultations, workshops, forums, and other means;
3. Examine the laws and regulations that may apply to mobile commerce in other regions of the world;
4. Fund research into the impact of mobile commerce on consumers, particularly those who are disadvantaged or vulnerable, such as children and low-income people. This research must be undertaken in a transparent, independent, and scientific manner;
5. Implement laws and regulations that are consistent and that:
    - Protect consumers from unauthorized transactions and provide cooling-off rights for situations where, for instance, consumers have purchased goods or services that have not yet been delivered, or where required disclosures have not been made;
    - Enable consumers to refuse payment or demand refunds for disputed charges without fear that their mobile accounts will be terminated;
    - Require vendors to take steps to ensure that purchases cannot be made by children without their parents' knowledge and consent;
    - Require clear and full disclosures about the products and services offered, the cost, and the terms and conditions in any commercial communication as well as immediately before any individual transaction;
    - Prohibit fraud and deceptive and misleading solicitations, and provide especially strong sanctions against such solicitations targeting vulnerable consumers;
    - Give special protection to children and restrict marketing practices targeting children;
    - Prevent unsolicited advertisements for products and services from being sent to consumers' mobile devices;
    - Provide effective and consistent payment dispute rights;
    - Provide consumers with the right to terminate any subscription of premium content or services with short notice;
    - Prohibit types of mobile commerce activities, such as gambling, based on the applicable laws of their respective countries;
    - Require that consumers' financial information is secured against external and internal abuse;
    - Protect consumer privacy in mobile commerce and prohibit use of any personal data (including purchase and location information) for purposes that consumers have not explicitly agreed to or that unfairly disadvantage them.

TACD further resolves that the EU and US governments should:

Encourage mobile commerce vendors, billing and payment intermediaries, and other businesses involved in mobile commerce to develop best practices and self-regulatory programs that:

- Provide effective means of authenticating purchasers to prevent unauthorized transactions;
- Provide clear disclosure of cancellation rights and policies, and easy means for consumers to cancel;
- Mitigate losses for unauthorized transactions by limiting the amount of charges that consumers may make in mobile commerce transactions within specific time periods and for single transactions;
- Give all mobile phone users easy and inexpensive means to block all premium content and services to mobile phones, including the ability for parents to do so on phones they intend to provide to their children;
- Help parents identify content that may be objectionable for children through the use of uniform pictograms;
- Provide effective means for consumers to resolve disputes concerning mobile commerce;
- Set reasonable policies based on applicable laws in the countries in which their customers reside for the types of products and services that will be offered in mobile commerce and for which billing services will be provided;
- Prevent fraud and deception through careful screening of vendors for whom services will be advertised and billing services will be provided;
- Set good standards for advertising that will ensure clear and full disclosures;
- Prevent unsolicited marketing for mobile services and enable consumers to easily exercise their rights not to receive such solicitations;
- Protect the security of consumers' financial information through use of encryption and other technical measures, and by implementing effective internal security measures;
- Protect the privacy of consumers' personal information and refrain from using it for purposes that consumers have not explicitly authorized or for purposes that unfairly disadvantage them.

***

European Commission Services' Response

In many respects, most of the issues raised in the recommendations do not concern exclusively those transactions carried out using a mobile phone, but could apply to all electronic commerce transactions and, in some cases, even to distance sales. In this respect, a wide range of Commission initiatives which are not specifically aimed at regulating mobile commerce can nevertheless contribute to reinforce the position of the consumer in this context.

In the field of electronic communications, the interest of consumers is of great importance to Commission policy actions. Making ICT products and services more accessible is an economic, social, ethical and political imperative. In this context, DG Information Society and Media, associated with DG Health and Consumer Protection, launched in January 2006 a general study to support the Commission i2010 initiative by analysing the origins as well as the impacts of the current lack of consumer's confidence in the information society products and services.

More specifically, a certain number of specific actions already address some of the concerns expressed in the TACD recommendations. This is the case, for instance, for those initiatives aimed at dealing with consumers' privacy concerns. In this respect, certain practices such as 'traditional' email spam, unsolicited electronic communications by mobile phone for marketing purposes are in principle 'banned' by the e-Privacy Directive (2002/58/EC) subject to limited exceptions. While mobile users have suffered less than email users so far, technology and

services convergence are expected to bring more mobile spam to users in the near future. In this context, self-regulatory efforts have long been called for by the Commission (see the 2004 Communication on unsolicited commercial communications 'spam'[12]). Recent efforts by industry should be welcomed in this regard[13]. Mobile spam messages misleadingly inciting consumers to call premium rate services are particularly worrying, but, generally speaking, these practices are covered by existing consumer protection and/or cybercrime law (e.g. Unfair Commercial Practices Directive 2005/29/EC, Framework Decision 2002/222 on Attacks against information systems), as confirmed by the workshop on premium rate services organised this year by the European Commission.

The consumer regulatory framework is also relevant to mobile commerce. For instance, although it contains no provisions specific to mobile commerce per se, the provisions of the distance selling directive 97/7/EC need to be taken into consideration when "mobile trading". The directive includes rights and obligations such as the provision of comprehensive information prior to the contract; confirmation of that information in a durable medium; the consumer's right to withdraw from the contract within at least 7 working days. However, the Commission realises that some of the provisions of the directive may need to be brought up to speed because of the emergence of new commercial practices such as mobile commerce. The Commission is therefore currently reviewing the distance selling directive alongside seven other consumer protection directives. In the course of this review, the Commission will examine whether consumers are adequately protected in the field of mobile commerce. Questions such as on which support should prior information be provided, how to confirm information in writing or another durable medium, should exemptions to the right of withdrawal be reconsidered in the context of mobile commerce, will be raised in the context of the review. The protection of minors will also be given consideration. An implementation report on the distance selling directive is planned in the early summer. A further Commission communication on the review of the EU consumer protection legislation at large is planned in the autumn.

The Data protection directive also requires that data can be used only for the purpose for which they have been legally collected. In any case, the person concerned is required to express his/her prior and unambiguous consent, i.e. informed and freely given consent to such processing in the mobile commerce.

More specifically, the e-Privacy Directive (2002/58/EC) provides for safeguards for the further use of location data generated by the use of mobile phones. In particular, such location data may only be used with the consent of the subscriber. Moreover, it should remain possible for subscribers and users, even if they have subscribed to a location-based service, to temporarily block the tracing facility. The Commission has supported the efforts of Article 29 of the Data Protection Working Party in this area. In November 2005, the latter Working Party adopted an Opinion on the use of location data with a view to providing value-added services (WP 115). The document provides for guidance, in particular on consent and information requirements[14].

Furthermore, since privacy enhancing technologies would allow a better implementation of the Data protection directive, the European Commission intends to call upon enforcement authorities to prevent software and hardware products, including consumer electronics, being built in a way that impairs compliance with the data protection legislation.

---

12 COM (2004)28)

13 See e.g. GSMA Mobile Spam Code of Practice, February 2006

14 The document is available on : http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf

The e-Privacy Directive is subject to the 2006 review exercise of the current regulatory framework for electronic communications and therefore also included in the public consultation carried out to prepare it[15]. The Commission is now reflecting on the various contributions received and plans to adopt a Communication setting out its view on the review which will be also subject to public consultation before the Commission adopts legislative proposals around the end of 2006.

It should also be noted that the European Commission has launched a discussion on the issues raised by the use of mobile phone services by children, in the framework of the Safer Internet Forum[16]. A plenary session of this Forum and a workshop were organised in 2005 on this issue[17]. It gathered mobile operators, content providers, industry representatives, child safety associations and public bodies and contributed to improve the common understanding of the risks and necessary actions at European level.

A survey of the existing national regulatory and self-regulatory frameworks was conducted in 2005 and it is available on the safer internet website[18]. In 2006, the European Commission has continued to support self-regulation and exchange of best practices (including parental control tools and labelling) in this area and to raise awareness among parents and children through the Safer Internet Plus programme[19]. Further discussions have been held to reach an agreement with mobile networks operators on best practices and their implementation across Europe. A document to be published for consultation is in preparation.

Finally, building on past initiatives, such as the Recommendation (97/489/EC) providing for the protection of customers using electronic payment verification instruments, the European Commission adopted in December 2005 a proposal for a Directive on payment services in the internal market[20], which applies, under certain conditions, to the execution of payment transactions by any means of communication at a distance such as mobile phones or other digital or IT services. The proposed Directive will increase and standardise rights and obligations for providers and users of payment services in the EU, with a strong emphasis on a high level of consumer protection. This includes mandatory/default execution time of one day for payments, the liability of the payment provider for correct execution, and a guarantee of full and timely payment.

15 http://europa.eu.int/information_society/policy/ecomm/tomorrow/index_en.htm
http://ec.europa.eu/information_society/policy/ecomm/info_centre/documentation/public_consult/review/index_en.htm

16 http://europa.eu.int/information_society/activities/sip/si_forum/index_en.htm

17 Presentations are available at
http://europa.eu.int/information_society/activities/sip/si_forum/mobile_2005/index_en.htm

18 http://europa.eu.int/information_society/activities/sip/si_forum/mobile_2005/country_reports/index_en.htm

19 http://europa.eu.int/information_society/activities/sip/programme/index_en.htm

20 COM 2005 603 final

Recommendations to the 2005 U.S.-EU Summit

May 10, 2005

(this is limited to the recommendations – for the letter sent to the Presidents, go to www.tacd.org/docs/?id=273, and for TACD's follow-up letter following the Summit, go to www.tacd.org/docs/?id=278)

We have already submitted detailed recommendations with regard to renewing the U.S.-EU economic relationship (www.tacd.org/docs/?id=267), but this Statement to the 2005 Summit is intended to focus on a few key ideas that can be fed into your discussions, with each other and with us, before and during the June 20th Summit in Washington D.C.

Process

TACD was very welcoming of the stakeholder consultations run by the U.S. Government and the European Commission, and urges you to take this open consultative approach forward into the new framework for transatlantic economic relations to be launched at this Summit.

The new open process that we endorse is a fresh working dynamic that should encompass two key principles. It should be a process where activities geared toward regulatory cooperation are nominated and discussed in a democratic and accountable fashion with a balanced group of stakeholders. It should also be a process with clear avenues for public input and transparent methods of decision-making and record-keeping. We urge you to allow opportunities for a balanced group of stakeholders and technical experts to obtain observer status so that they may listen to and participate in substantive discussions. Such a system, by including stakeholders as observers, leads to both broader public acceptance of agreements and better outcomes to discussions.

Rather than limit the TEP goal to creating a "barrier-free marketplace", turn that vague and unhelpful concept on its head. Instead, develop a process for identifying and emulating "best practices" on both sides of the Atlantic. Regulations to prevent fraud, and ensure public health and safety, foster confidence in the integrity and fairness of the marketplace. They should not be seen as barriers to trade, but as critical components of consumer confidence that will encourage trade, online purchases, and other economic activity.

Here are four areas in which TACD would like to see the U.S. and EU working together to encourage consumer confidence in the transatlantic economy:

Diet-related disease

The time is ripe for U.S.-EU discussions on best practices to effectively tackle the problem of diet-related disease. People in both areas of the world suffer from the same diet-related diseases, and often the same multi-national food companies market the same types of products on both sides of the Atlantic.

The TACD urges the U.S. government to follow the lead of the EU regarding the establishment of the EU Platform on Diet, Physical Activity, and Health, which has asked for commitments from all relevant stakeholders. We support this approach from the European Commission to use all of the tools available to it, if industry fails to take adequate measures on a voluntary basis within a reasonable time period. These tools include mandatory regulation, which we suggest could be used in relation to controls over the way foods are marketed to children, for example.

Both the U.S. and the EU should base policies on the World Health Organization's Global Strategy on Diet, Physical Activity, and Health. The Global Strategy states that food marketing and advertising to children, food composition, fiscal measures, agricultural subsidies, food labeling, mass communication campaigns, and other factors all play a role in this public health problem.

The Transatlantic Economic Partnership explicitly states that there is an objective to strengthen regulatory cooperation in the field of health; the U.S. and EU should thus engage in a system of "best practices" to actuate this objective.

European Commission Services' Response

The objective of the EU Platform on Diet, Physical Activity and Health is to catalyse voluntary action across the EU by business, civil society and the public sector. Members of the Platform include the key EU-level representatives of the food, retail, catering, and advertising industries, consumer organisations and health NGOs.

The Platform is to provide an example of coordinated but autonomous action by different parts of the society. It is designed to stimulate other initiatives at national, regional or local level, and to cooperate with similar fora at national level. At the same time, the Platform can create input for integrating the responses to the obesity challenge into a wide range of EU policies. The Commission regards the Platform as the most promising means of non-legislative action, as it is uniquely placed to build trust between key stakeholders. If the Platform does not deliver results, the Commission will consider other measures.

A transatlantic conference hosted by the European Commission in the framework of the European Platform for Action on Diet, Physical Activity and Health took place in Brussels on 11 and 12 May 2006.

The purpose of this conference was to help to identify good practice through an exchange of ongoing and new strategies and initiatives on diet, physical activity and health between the main EU and U.S. players (i.e. public and private sectors, consumer groups, health non-governmental organisations, food and advertising industries, regulators, and researchers). The event provided ideas for improving existing actions of the EU Platform; gave the basis for future transatlantic cooperation on topics such as food advertising, food labelling and reformulation, consumer education and research (consumer behaviours, causes of obesity; preventative factors); and, paved the way toward common objectives between the EU and the U.S. Representatives from EU and US consumer organisations participated in the conference.

The Platform is primarily action-based, based on already established facts but in some areas the Platform members have committed themselves to more research-related actions, as for example the commitments from industry to promote consumer research to improve the understanding of what kind of educational messages will best promote balanced diets and healthy lifestyles; to explore the possibility for relevant stakeholders to undertake a study on the diverse causes related to obesity (socio-economic factors, family changes, etc); how best to promote effective interventions to help maintain appropriate and balanced eating habits and to influence consumer behaviour towards healthy eating.

There is a need to better disseminate results of projects, including EU funded projects in the area of food research. Key research areas and actions should be identified that allow for participation from the whole community, including industry. Research on consumer behaviour, including how consumers perceive and deal with information, is important in addition to food science-related research.

Privacy and Security Standards

Consumer confidence in online and offline transactions, domestic and cross-border, is increasingly eroded by problems and criminal activities in the digital environment. One example is "phishing," in which identity thieves steal people's personal information by sending spam pretending to be from legitimate businesses. Another is theft of customer information due to inadequate business security measures. The burgeoning use of radio frequency identification devices (RFID) in consumer goods and government documents also raises concerns about the ability to track and trace personal information without the subject's knowledge or consent, and without limitations of use or adequate protection from unauthorized access.

TACD believes that the U.S. and EU should work towards a common framework on consumer privacy and security in the digital environment that provides effective legal rights and means of redress. Consumers' concerns should be taken into account early on when new technologies such as RFID are developed. All stakeholders, including consumers, should be consulted in the process of developing upwardly harmonized policies for addressing these issues. The U.S. and EU must also increase their efforts to implement effective cross-border enforcement mechanisms.

Common approaches to best-practice regulation in the digital environment helps to build consumer's trust in new technologies, spurs business as it fosters the demand side of the market, and helps companies to standardize their risk management and other processes.

European Commission Services' Response

Concerns specifically related to the use of radio frequency identification devices are addressed in the specific section devoted to this mater of the present contribution. This response addresses the remaining elements.

Providing trust to the user or consumer is a complex task that requires a number of combined initiatives. In tackling security challenges for the Information Society, the European Union has developed a three-pronged approach embracing specific network and information security measures (which aim at guaranteeing the stability of the electronic communication networks which are used to provide services to consumers), the regulatory framework for electronic communications (which includes privacy and data protection issues) and the fight against cybercrime.

Firstly, the Communication "i2010 – A European Information Society for growth and employment"[21], highlighted already the importance of network and information security for the creation of a single European Information space. In this line, a forthcoming Communication will present this year the Commission's strategy for a Secure Information Society, taking into account all developments since the Communication "Network and Information Security: proposal for a European Policy approach"[22]. The Communication will, therefore, review the current state of threats to the security of Information Society, the technical and legislative developments with a view to determine what additional steps should be taken to improve network and information security. The planned security policy would also take into account the key role of the European Network and Information Security Agency (ENISA)[23], established in 2004, that contributes to the development of a culture of network and information security for the benefit of citizens, consumers, enterprises and public sector organisations throughout the European Union.

21 COM(2005) 229 final
22 COM(2001) 298 final
23 See: http://www.enisa.eu.int/

Secondly, the regulatory framework for electronic communications, currently under review, includes security-related provisions. In particular, the Directive on privacy and electronic communications[24] contains an obligation for providers of publicly available electronic communications services to safeguard the security of their services. In addition, provisions against spam and spyware are also laid down. Building on the 2004 Spam Communication, a new specific Communication addressing spam, spyware and malware issues is expected in 2006. As regards consultation, the 2006 review of the e-Privacy Directive provides for various opportunities for all stakeholders to express their views. The Commission would welcome an active participation of consumers in the consultation process.

Thirdly, an additional communication on cybercrime issues will also be adopted this year by the Commission.

However, legislation is not enough and effective enforcement, technical solutions, self-regulation and user's awareness are indispensable.

The Commission considers that the use of appropriate technological measures is an essential complement to legal means and should be an integral part in any efforts to achieve a sufficient level of privacy protection. Products, applications and systems should not only be developed in compliance with the applicable data protection rules but also in a privacy enhancing manner whenever possible. By adding safeguards to the level of compliance with data protection legislation, consumers will have more trust in e-commerce and will enjoy more of its benefits.

But the key issue is not only how to create technologies that are really privacy enhancing, but how to make sure that these technologies are properly identified and recognised as such by the users. Some sort of certification schemes may play a crucial role and the Commission will continue to follow developments in this area. The Commission believes that such schemes should indeed be encouraged and further developed. The objective is not just better privacy practices, but also to increase transparency, and therefore the trust of users, and to give those investing in compliance and even enhanced protection an opportunity to demonstrate their performance in this respect and exploit this to their competitive advantage.

The Commission intends to support further developments of privacy enhancing technologies and promote their use and adoption by, amongst other means, supporting, funding or co-funding research and raising information awareness by organising a series of EU-wide debates, targeted conferences and dedicated workshops.

Finally, trust and security also play an important part in the programmes of the European Union devoted to research and development. The 6th Research Framework Programme addresses these issues through a wide range of projects. Security-related research is planned to be reinforced in the 7th Framework Programme with the establishment of a European Security Research Programme (ESRP)[25]. In addition, the Safer Internet Plus programme supports networking projects and the exchange of best practices to fight against harmful contents circulating on information networks.

[24] Directive 2002/58/EC

[25] The ESPR is being prepared by a Preparatory Action for Security Research during the period 2004-2006.

Intellectual Property

Governments on both sides of the Atlantic need to address overreaching and abuses in the areas of intellectual property rights, rather than promoting ever-increasing levels of protection. We are particularly concerned that new digital rights management systems and technological protection measures are eroding the rights of consumers, and presenting profound barriers for access to knowledge goods. The problems facing consumers should be addressed by the U.S and EU in the World Intellectual Property Organization (WIPO) Standing Committee on Copyright.

We are also concerned about the proposed treaty on the protection of broadcast and webcasting organizations, and urge that the U.S. and EU seek public comments on the following issues: what impact will the treaties have on the public domain, and on owners of copyrighted works?; and should the treaty create a new layer of intellectual property protection on Internet transmissions? In the area of medicine, we call upon governments to evaluate the proposal for a new trade framework for medical R&D, as a substitute for bilateral agreements on drug prices or patents (www.tacd.org/docs/?id=272).

European Commission Services' Response

See Commission response on Digital Rights Management, page 10, § 6

Regulating Industrial Chemicals

The U.S. government should end its effort to weaken the EU's precautionary approach to regulating chemicals, called Registration, Evaluation, Authorisation and Restrictions of Chemicals (REACH). TACD considers REACH to be a significant advance in consumer protection over U.S. chemical policy. We call on the U.S. to emulate, rather than undermine, the EU approach. We call on the EU to give serious consideration to TACD's proposals for strengthening REACH by focusing on the most hazardous chemicals (for which there should be no volume threshold) and incorporating the principle of substitution.

We therefore urge the EU and U.S. to take a cooperative, rather than adversarial, approach to the real problems of hazardous chemicals and chemical pollution for public health, safety and the environment. A new model of regulatory cooperation focusing on balanced stakeholder participation and best practice would provide an opportunity for regulators to learn about the strengths and weaknesses of each other's systems. For instance, the EU and U.S. could share emerging data on hazards of chemicals that may be available on one side of the Atlantic, but not the other. This should result in a system of regulating chemicals that better protects the consumer on both sides of the Atlantic.

European Commission Services' Response

Strengthening REACH by focusing on the most hazardous chemicals (for which there should be no volume threshold)

For the most hazardous chemicals, volume thresholds are, in fact, not used in the case of authorisation or restrictions. Substances that are of very high concern (carcinogenic, mutagenic and reprotoxic (CMR), persistent, toxic and bioaccumulative (PTB) and very persistent and very bioaccumulative (vPvB), and substances of equivalent concern) can be subject to authorisation, regardless of the volume of production or import.

As regards registration, however, volume thresholds are used as the criteria for the identification of the applicable requirements. REACH prioritises and categorises substances on the basis of production or import volumes, starting at 1 tonne per year. This means that production and import volumes are used as an approximation of exposure, something that is not new: this is the approach behind, for example, the OECD work on chemicals, which focuses on high production volume chemicals. This also helps to ensure that the impact of REACH is proportionate, as low volume substances might be rendered unprofitable if testing requirements were too extensive.

The registration process is tiered to prioritise the substances most likely to be of the greatest concern. Phase-in substances manufactured or imported in volumes at or above 1000 tonnes/year as well as those that are classified as CMR, categories 1 and 2, have to be registered within 3 years after the entry into force of the Regulation. However, some information, which is normally required for a registration process, can be omitted if there is no exposure. This finetunes the requirements based on the uses of the substance.

As regards the substances that fall within the 1-10 tonnes category, the Political Agreement reached by the Council on 13 December 2005 introduces further elements for prioritisation. This means that a full data-set required for prioritised substances in their 1-10t range has to be provided as set out in Annex V of REACH. Prioritised substances are substances for which there are indications that they could be CMR, PBT or vPvB, or which fall in the category of "non-phase-in" substances.

In addition, a complete Annex V data-set is also necessary for the registration of substances that are classified as dangerous for health or the environment and that have wide-spread or diffusive uses. For all other cases, substances in the 1-10t range can be registered only on the basis of a set

of data that includes some defined physicochemical information and any other available and relevant information.

The approach proposed by TACD would force authorities to assess the hazard of chemicals based on very limited knowledge.

It should be recalled that each of the existing QSARs[26] has a limited field of application and is validated for substances with certain types of structure only. In other words, it is by no means certain that such a screening would catch the most dangerous substances.

Furthermore, the proposed approach would put the burden of proof back on the public authorities, making the system *de facto* unworkable. The authorities would in fact have to prove the risks of a chemical substance before full registration could take place. Such a system would be difficult to enforce. In contrast, REACH gives the burden of proof to industry to assess the safe use of the chemicals they produce, use and place on the market. This reversed burden of proof is one of the cornerstones of the REACH approach.

Incorporating the principle of substitution

The provisions of REACH will stimulate the demand for safer substances and technologies[27], remove obstacles to the development of alternatives and promote the introduction of new, less risky substances on the market. REACH will encourage and promote substitution by making safer substances more attractive for commercial reasons. Thanks to increasing information about substances, downstream users of chemicals will be able to make informed decisions on the substances they use in their products and will be able to pursue low-risk strategies.

The Political Agreement by the Council has introduced the requirement for all applications for authorisation to contain an analysis of substitutes to be carried out. This will mean applicants will have to assess the possible substitutes for their substance before applying for an authorisation.

Nevertheless, REACH remains an essentially risk-based system and so the adequate control of risk must be a prime consideration in granting authorisations.

Sharing emerging data on hazards of chemicals.

One of the aims of REACH is to provide information on the properties of substances, and a lot of this information will be available free on the website including:

→ the classification and labelling of the substance;
→ physicochemical data concerning the substance and pathways and environmental fate;
→ the result of each toxicological and ecotoxicological study;
→ any derived no-effect level (DNEL) or predicted no-effect concentration (PNEC).

In addition, "robust study summaries" or "study summaries" that were registered for a substance will also be available on the website, unless the registrant can justify why they should be regarded as confidential.

---

26 Quantitative Structure-Activity Relationships

27 PA recital (7): an important objective of the new system to be established by this Regulation is to encourage and in certain cases to ensure that substances of high concern are eventually replaced by less dangerous substances or technologies where suitable economically and technically viable alternatives are available.

Moreover, Article 103 allows the management board of the future Chemicals Agency, in agreement with the relevant Committee or the Forum, to invite representatives of 3rd countries to participate in the work of the Agency. These provisions provide a good basis for sharing information on the hazards of chemicals.