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 (page 2)
- Radio Frequency Identification (RFID) (page 2-3)
- Digital Rights Management (pages 4-5)
- Broadcasting Rights Treaty (page 5)
- Mobile Commerce (pages 6-7)
- Recommendations to the 2005 U.S.-EU Summit (pages 7-9)

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.

***

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.

***

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.

***

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.

***

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.

***

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.

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.

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).

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.