



GLOBAL ADVERTISING LAWYERS ALLIANCE

Marketing Abroad:

Navigating International Regulation of Direct Marketing and Privacy

Target 'Europe':

*A few things to know about Home Shopping and Data Protection
(as of February 2004)*

By:

Avv. Felix Hofer

Hofer Lösch Torricelli - www.hlrlaw.it

Member for Italy of GALA - www.gala-marketlaw.com

The Legal Framework

Even though it's been conceived as a common internal market and it's governed by a legal framework (Directives and Regulations) issued with harmonizing intents, the European Union still suffers from significant differences between Member States as to regulation of industry and business sectors.

The expansion process, which in the next years will bring into the Union more than ten new member states, is not likely to contribute to "the smoothing of the edges". Such development will rather stress the existing, broad range of differences between Member States, which currently may be recognized as a result of combining together areas characterized by cultural and social differences, established within the context of a longstanding past of distinctions.

Nevertheless the so-called "Community Law" (i.e. the Directives and Regulations issued by the EU) should be taken into due account as an important information source for all those intending to target Europe with their businesses. In fact, Community Law deserves proper consideration as a reference context for in-advance discovery of critical areas, of problems likely to arise and of obstacles apt to result in barriers to successfully performing business in Europe. Frequently it also may offer viable solutions for overcoming difficulties and barriers.

Therefore companies, not having branch offices or subsidiaries within the territory of the EU, should always focus on achieving at least a rough idea about the general principles and legal provisions, that will become applicable (to) or relevant (for) their business activities, when doomed to target European customers.

Direct Marketers should deserve particular attention to some key provisions governing on-line sales and personal data handling always involved by such business.

(a) Home Shopping

Relevant EU Provisions:

(1) The 'Doorstep Selling' Directive (= Council Directive no. 85/577/EC):

Applies primarily to B2C relations, i.e. contracts for supply of goods or services concluded,
- while the trader is away from his place of business, or
- during an unsolicited visit by a trader to the consumer's home or to the consumer's place of work,
- during visits requested, if the consumer did not know that the supply of those other goods or services were a part of the trader's commercial or professional activities when the visit was asked for.

Obliges traders to provide consumers with proper, written notice about their right of rejection or repudiation

Grants consumers the exercise of their right of rejection within a period of seven days from the notice

Establishes that exercise of this right of repudiation or rejection is governed by national law

Does not permit consumers to give up their right to repudiation and allows Member States to adopt or keep in force legislation which is more sympathetic to consumers than the Directive's rules

(2) The 'Distance Selling Directive' (= Council Directive no. 97/7/EC):

Harmonizes domestic laws concerning distance selling contracts between consumers and traders (or suppliers), i.e. contracts concluded without a face to face meeting

Applies to sales performed through technical means, as radio, telephone, television, fax and home computer (in that context covers also junk mail and press advertising)

Puts onto the traders specific information requirements (e.g. about cost, delivery and performance obligations)

Grants consumers the right to cancel the contract by notice (cancellation periods are fixed in the Directive) and requires consumers canceling the contract to return any goods delivered

(3) The 'TV Without Frontiers' Directives (= Council Directive no. 89/552/EC, amended by Council Directive no. 97/36/EC)

Those directives are relevant in this context, because they contain provisions covering promotion, distribution and production of television programs and marketing aspects, as: advertising, sponsorship, and protection of children and young people

In particular such provisions refer to: broadcasting time dedicated to commercials, placement of ads and program interruptions admitted, restrictions as to advertising for certain products or targeted to a specific public,

Apply also to the content of audio-visual services

Also deal with important side aspects as jurisdiction (country of destination principle), transmission time reserved to European works/events/content, safeguarding the media and information industry, protection of fair competition (through provisions aimed to avoid the abuse of a dominant position)

(4) The 'E-Commerce' Directive (= Council Directive no. 2000/31/EC)

Focuses on assuring the correct functioning of the Internal Market (by ensuring free movement of information society services – ISS - between the Member States, but

Does not cover:

- Use of ISS by a consumer while on the premises of a trader,
- Services with a 'material content' (e.g. which dispense a cinema ticket),
- Services involving physical delivery of products (e.g. E-Bay, Amazon),
- Services provided by fax or phone, or simultaneously to an unlimited number of users (e.g. broadcast TV),
- Other areas, as VAT, betting, gaming and lotteries.

Establishes for 'Service Providers', supplying information society services, jurisdiction according to the 'country of origin' principle,

Requires Service Providers to deliver specified information in a tone "easily, directly and permanently accessible", to acknowledge the receipt of orders and to empower customers to correct input errors.

(b) Data Processing

Marketing – just as a broad range of other services present in businesses performed on-line – necessarily implies collecting, storing, handling, transferring, profiling, in other terms, "processing" of personal data, by different subjects, as for e.g. Agencies, Advertisers, Media Companies, Others (IPs, Call Centers, Research and Fulfillment Companies), which subsequently involves specific liabilities for those subjects.

Relevant EU Provisions:

(5) The Directives on 'Privacy and Electronic Communication' (= Council Directives no. 95/46/EC & no. 2002/58/EC)

Aimed at establishing a common legal framework for the protection of data privacy,

To this purpose *Directive 95/46/EC* sets as general key principles, directed to govern the conditions for legitimate handling of information on persons, that their data may be processed:

- only fairly and lawfully,
- just for specified purposes and not for other uses, except – under observation of appropriate safety measures - for historical, statistical, or scientific purposes,
- on condition that their handling results adequate, relevant, and not excessive in relation to the purposes for which they are collected,
- as long as they're kept correctly, in accurate, complete and updated form, and are stored only for the period necessary for the stated purpose (longer storage for historical, statistical, or scientific purposes requires 'anonymization'),
- provided that the 'data controller' gives proper notice to the 'data subject' as to the following information: (a) controller's identity (or that of its local representative), (b) intended purposes for the processing, (c) categories of data processed, (d) recipients of the data, (e) consequences of not submitting requested data, (f) rights of access to collected data and of correction of their content,

As to legitimacy of the handling, the Directive holds that personal data may be processed:

- either after achieving data subject's "unambiguous consent",
- or when necessary:
 - for performing a contract,
 - for compliance with a legal obligation to which the controller is subject,
 - in order to protect the vital interests of the data subject,
 - for the performance of a task carried out in the public interest or in the exercise of official authority,
 - for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed (except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject),

Particularly strict provisions regulate:

- processing of so-called 'sensitive data' (i.e. data revealing: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life),
- data transfer from EU member states to third countries (the 'Safe Harbor' agreement between the EU and the US covers this area,

For grounds of public interest the Directive contains also exemptions from the above-mentioned regime, e.g. for reasons of national security, defense, public security, crime prevention, detection and prosecution, important economic or financial interests of a member state or of the EU (as monetary, budgetary and taxation matters), monitoring, inspection or regulatory functions connected with the exercise of official authority.

Directive 2002/58/EC dated July 12th, 2002 (in force since November 1st, 2003 and abolishing the previous *Directive 97/66/EC* of December 15th, 1997 on personal data processing and privacy protection in the telecommunications sector) intends to ensure "an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector as well as the free movement of such data and of electronic communication equipment and services in the Community",

The Directive's general principles are focused on creating a common legal framework with respect to certain procedures of data handling performed through electronic means and other recently developed technologies,

Among the most relevant aspects of the new provisions it may be considered that:

- the use of cookies and other invisible tracking devices, apt to collect personal data on the Internet, is allowed if the targeted data subject is granted: proper notice about the information stored, its purpose and the period of retention as well as an option for acceptance, rejection or choice on the information to be released,
- location data generated by mobile phones can only be further used or passed on by network operators with explicit user consent (an exception applies as to data transfer to emergency services and to law enforcement authorities),
- electronic mailing for direct marketing purposes – including SMS or other electronic messages sent to mobile or fixed terminals - requires specific prior consent by the targeted data subject (“opt-in” option).

(6) The ‘Anti Money Laundering’ Provisions (= Council Directive no. 91/308/EC – issued on June 10th, 1991 – and Directive no. 2001/97/EC, dated December 4th, 2001, to be implemented by June 15th, 2003)

Originally *Council Directive 91/308/EC* was targeted to ‘credit and financial institutions’, requiring them to assure “*identification of their customers by means of supporting evidence when entering into business relations, particularly when opening an account or savings accounts, or when offering safe custody facilities*”; such identification requirement did also apply to “*any transaction with customers ... involving a sum amounting to ECU 15 000 or more, whether the transaction is carried out in a single operation or in several operations which seem to be linked*”,

In the following, *Directive no. 2001/97/EC* has extended those identification requirements also to “*legal or natural persons acting in the exercise of their professional activities*” and specifically to (among others) “*auditors, external accountants and tax advisors, real estate agents, notaries and other independent legal professionals, when they participate, whether:*

- (a) *by assisting in the planning or execution of transactions for their client concerning the:*
 - (i) *buying and selling of real property or business entities,*
 - (ii) *managing of client money, securities or other assets,*
 - (iii) *opening or management of bank, savings or securities accounts,*
 - (iv) *organization of contributions necessary for the creation, operation or management of companies,*
 - (v) *creation, operation or management of trusts, companies or similar structures,*
- (b) *or by acting on behalf of and for their client in any financial or real estate transaction ... ”.*

Therefore, professionals have now to consider properly that:

- all institutions and persons subject to the particular provisions are held to “*require identification of their customers by means of supporting evidence when entering into business relations*”,
- in cases in which it appears (even as a mere doubt) that actions is taken on behalf of third parties, “*reasonable measures*” must be taken in order “*to obtain information as to the real identity of the persons on whose behalf those customers are acting*”,
- such “*reasonable measures*”, aimed at achieving the required identification, “*shall ensure that the customer's identity is established, for example, by requiring additional documentary*

evidence, or supplementary measures to verify or certify the documents supplied, or confirmatory certification by an institution subject to this Directive, or by requiring that the first payment of the operations is carried out through an account opened in the customer's name with a credit institution subject to this Directive”,

- in addition, all the institutions and persons subject to the Directive are called to “*keep the following for use as evidence in any investigation into money laundering:*

— *in the case of identification, a copy or the references of the evidence required, for a period of at least five years after the relationship with their customer has ended,*

— *in the case of transactions, the supporting evidence and records, consisting of the original documents or copies admissible in court proceedings under the applicable national legislation for a period of at least five years following execution of the transactions”*,

Finally the Directive also recommends “*Member States shall ensure that the institutions and persons subject to this Directive and their directors and employees cooperate fully with the authorities responsible for combating money laundering:*

(a) by informing those authorities, on their own initiative, of any fact which might be an indication of money laundering,

(b) by furnishing those authorities, at their request, with all necessary information, in accordance with the procedures established by the applicable legislation”.

(c) Coming up

(7) The Directive Proposal on ‘Services in the Internal Market’ (as per January 2004)

This Directive (thought to take full effect by 2010, while national implementation should be assured within 2 years after the Directive’s adoption) is meant to cover quite a broad range of activities (save financial services, electronic communication, taxation, postal services, energy sources’ distribution), such as: ***business services*** (e.g. management consultancy, certification and testing, facilities management including office maintenance and security, *advertising*, recruitment services - i.e. employment agencies, services of commercial agents- and ***services provided both to businesses and to consumers*** (e.g. legal or fiscal advice, real estate services – i.e. estate agencies, construction including the services of architects - transport, distributive trades, the organization of trade fairs, car rental, travel agencies, security services; and consumer services, as tourism, audio-visual services, leisure services, sports centers, amusement parks, as well as health and healthcare services or household support services, e.g. help for the elderly),

It should be applied to services requiring the proximity of provider and recipient, as well as to services requiring travel by the recipient or the provider and services provided through distance means, including the Internet,

The Directive is aimed at granting, by creating a harmonized legal framework, the elimination of existing obstacles to freedom of establishment for service providers (where ‘*service*’ means any self-employed economic activity, while ‘*provider*’ has to be read as any natural person who is a national of a Member State, or any legal person, who offers or supplies a service) and free movement of services between the Member States, through:

– *simplified administrative measures*, particularly involving the establishment of "single points of contact", at which service providers can complete the administrative procedures relevant to their activities, and offering the possibility of handling all relevant procedures by electronic means,

- *uniformed authorization/licensing schemes*, applicable to service activities and concerning the conditions/procedures for obtaining an authorization;
- *the prohibition of particularly restrictive legal requirements*, currently in force in certain EU Member States (e.g. discriminatory requirements based directly or indirectly on nationality or, with regard to companies, the place of its registered office, limitations as to establishing branch offices, agencies or subsidiaries in different Member States),
- *the adaptation* of certain other legal requirements currently applied by Member States with the conditions laid down in the Directive (e.g. with the principle of ‘proportionality’).
- *the application of the ‘country of origin’ principle*, according to which a service provider would become subject only to the law of the country in which he is established and Member States may not restrict services from a provider established in another Member State (derogations which are either general, or temporary or which may be applied on a case-by-case basis would be admitted);
- *the right of recipients* to use services from other Member States without being hindered by restrictive measures imposed by their country or by discriminatory behavior on the part of public authorities or private operators,
- *a mechanism to provide assistance to recipients* who use a service provided by an operator established in another Member State and - in case of posting of workers in the context of a service’s provision – to provide the allocation of tasks between the Member State of origin and the Member State of destination and the supervision procedures applicable.

With the purpose of increasing confidence and mutual trust between Member States, the Directive proposal also intends to achieve the following goals:

- *harmonization of legislation* in order to grant throughout the EU a satisfying level of equivalent consideration of matters of general interest (e.g. consumer protection with respect to the provider's obligations concerning: information, professional indemnity insurance, settlement of disputes, exchange of information on the service provider’s qualities/qualifications and after sale guarantees),
- *stronger mutual assistance between national authorities*,
- *measures for promoting the quality of services*, such as voluntary certifications, quality charters or cooperation between chambers of commerce or crafts’ associations,
- *promotion of codes of conduct*, prepared by interested parties at Community level on specific matters (e.g. commercial communications by the regulated professions).

Practical Experience: A close up on selected countries

Law and jurisprudence, in general, and legal regulation of single sectors, specifically, are obviously not immune from the negative impact derived from “different readings” of the Community Law’s provisions, due both to domestic reasons and habits as well as to differing interpretations rendered by national courts.

The sectors of Direct Marketing and Data Protection offer a good example of how local distinctions or domestic readings within what’s supposed to be a “common market” may display harmful side effects to cross-border business.

A snapshot on some differing national applications in some European countries of general principles, meant to supply a common legal framework throughout the EU, and on the different solutions sometimes delivered by European Courts for – apparently – identical problems/cases will eloquently demonstrate how careful foreign companies should be in approaching the European market, in order to successfully outflank still existing barriers to business and services targeted to a transnational public.

Germany:

In 2003 the court of Berlin (Landgericht – LG) was called to deal with a complaint about the receipt of an unsolicited commercial. The plaintiff had registered his cell phone number with an IS provider that was offering to its clients a free SMS messaging service. The provider had passed on such data – without the cell phone holder’s consent - to another company, which used it for running an advertising campaign performed via SMS.

In its decision (dated January 14th, 2003) the Court found that a violation of the data protection provisions occurred, issued a cease injunction against the two providers involved and fixed an eventual fine of 250.000 Euro for non compliance with the desist order. It also awarded 7.500 Euro as damage compensation to the plaintiff for the three unsolicited e-mails received.

The Court applied consolidated jurisprudence established with respect to unsolicited commercial messages in general to such practice performed by electronic means (the decision calls on the provisions set by Article 823 of the German Civil Code – BGB and Article 1 of the Unfair Competition Act – UWG).

Italy:

(1) A University Professor received an e-mail ad on an address, available on the University’s web site.

The recipient raised a complaint before the local Data Commissioner stating that his address was listed on the website “for institutional purposes” only. Therefore improper use of his personal data for commercial purposes occurred.

The advertiser’s defense was that the listing of the address in a ‘public’ directory (i.e. a University website) allows for public use of the data.

The Authority’s decision (June 24th, 2002): The fact that personal data can be found on the Net does not make it publicly available. Specific purpose pursued through Internet diffusion becomes relevant. In the case, addresses

available are only for a 'limited purpose' (the institutional one) and free use for e-mail sending was not allowed without prior consent.

(2) A bank's client, despite explicit denial of consent to commercial communications, regularly received, together with his statement of account, advertising material. The client asked that this sort of unsolicited mailing be stopped, however, as the bank insisted, a complaint arose with the Data Commissioner.

The Bank's defense stated that communications was sent for informative-educational purposes (i.e. to explain effects linked to introduction of the Euro), while the other – promotional – content had to be considered as just marginal and not likely to change the communication's main purpose significantly.

The Authority's decision (May 20th, 2002) was that the bank acted illegally by sending the promotional material to an address extracted from its business database, against the addressee's specific will.

In addition, the Authority transferred the case to the criminal prosecutor for evaluation of the bank's behavior (as illegal personal data processing may result in a criminal offence, punished with imprisonment up to 3 years). The verdict has still to be delivered.

United Kingdom

(1) On September 10th, 2003 the Advertising Standards Authority – ASA issued its first landmark decision with respect to the meaning of "specific consent" – under the new privacy regulation - required for using marketing lists and targeting consumers via e-mail campaigns.

A Southampton based seminar provider started an e-mail campaign sending messages with the following headline: "Business Seminars – Telesales & Selling Skills Made Easy". When opened, the message resulted to be directed to promoting "a selling sales course for non-aggressive people".

A complaint was filed with the ASA for infringement of the CAP code, raising two issues: (a) that from the e-mail's subject line it did not result clear that a marketing communication was the content of the e-mail, (b) no explicit consent from the addressee had been sought out – and received – before sending the message.

The ASA considered that the reference to "Business Seminars – Telesales & Selling Skills Made Easy" allowed to easily identify the message as a marketing communication, but also held that after March 2003 such communication could not be legitimately sent – not even to existing customers – without an explicit prior consent from the addressee. The defender's argument that a mailing list of subjects willing to receive promotional e-mails had been used was not considered as relevant.

(2) Very recently (on January 21st, 2004) the ASA had to deal with the following complaint (Media: E-mail - Sector: Leisure):

Objections to several e-mails for a prank telephone call service and for a CD ROM. The subject headers of the e-mails included, among others, the following: "Fun Prank Calls"; "Gags r US", "Unbelievable Secrets CD" and "Phone Jokes".

As to the text the e-mails contained statements as: "... This email has been sent to you as an opt-in promotion from a partner company, and has originated outside of the EU ..", ".. This promotion has been sent to you because you have opted to receive promotions from us or one of our partner companies. This email has been sent on our behalf and not actually by us, which has originated from the European Union ..", "... To exclude your email

address from future promotions, please call 0871 ...", "... If you would rather not hear about our promotions please call the list managers on 0871 ...". The telephone number changed on subsequent e-mails.

The complainants objected that:

- 1. the e-mails were sent unsolicited,
- 2. the claims "This email has been sent to you as an opt-in promotion from a partner company" and "This promotion has been sent to you because you have opted to receive promotions from us or one of our partner companies" were misleading,
- 3. the e-mails were not recognizable as advertisements until they were opened,
- 4. consumers who telephoned the number to be removed from the database were given a defunct free-mail address, and that the e-mails did not provide a way to opt out of receiving further messages.

The ASA considered all complaints grounded finding that:

- (i) the e-mails seemed to be sent either by or on behalf of the advertiser (who also failed to supply evidence apt to show that consumers had consented to receive the e-mails; on the other hand the Authority noted that the Independent Commission for the Supervision of Standards of Telephone Information Services - ICSTIS had fined the advertiser for sending promotional e-mails to business addresses),
- (ii) the advertiser did not respond on complaints no. 3 & 4, an attitude to be considered as a clear breach of the Code,
- (iii) furthermore, some of the subject headings did not make clear that the e-mails were advertisements,
- (iv) finally, consumers were not given the opportunity to opt-out of receiving future messages (a possibility to be granted on each occasion, i.e. for each e-mail received as to future messages).

(3) In December 2003 the same Authority was called to handle two other cases of unsolicited e-mail marketing:

(a) B... in B... a Bristol based company promoted business opportunities through an e-mail characterized by a very informal style and featuring nothing else but the word "Hi" in the subject line.

The ASA found that receivers of such e-mail could not become aware of the fact that a business opportunity was offered without opening the message. In addition it noted that the complainant was not a customer of the advertiser and that no prior consent had been sought before contacting the targeted person.

Therefore the ASA held that a clear breach of the Privacy Code's provisions occurred.

(b) E.....Tech....., one of UK's leading PC sellers, also promoted its products through e-mail marketing.

Recipients of unsolicited e-mails raised complained. The company defended its marketing campaign by assuming that it had used a database presented – and sold – by a third party as an opt-in address list, which only later on turned out not to be the case.

The Authority found that the company had failed to check whether the database's supplier had acted in bona fide or not. Again a breach of the provisions governing handling of personal data was found.

SWEDEN/EU

At the end of year 2003 the European Court of Justice (ECJ) delivered a sort of "milestone" decision with respect to the provisions of the Data Protection Directive on a case referred by a Swedish Court of Appeal.

The case originated from the following circumstances: a Swedish parish organized a computer course. Ms. L....., one of the participants to that course, was given the task of setting up an Internet home page and displayed - on a site created to that purpose – personal information about fellow church volunteers (i.e. names, addresses, phone numbers, jobs, hobbies, pro bono activities, etc.). Unfortunately the initiative came to the attention of the Swedish Data Protection Authority, which applied a fine (of approx. 500 USD) for illicit data processing (i.e. collecting

data without notifying the authority and transferring such data abroad without prior consent of the individuals involved). Ms. L.... opposed to the fine in front of a Swedish Court of Appeal, which decided to achieve an opinion of the ECJ in order to clarify the Data Protection Directive's correct reading.

The ECJ (judgment November 6th, 2003 in case C-101/01) disagreed with Ms. L...’s defense arguments and established the following principles on the Directive’s provisions:

1. “The act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data ..”
2. “Such processing of personal data is not covered by any of the exceptions in Article 3(2) of Directive 95/46” (the exemption referred to concerns data handling for purely personal or domestic activities),
3. “Reference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health...” and therefore involves revealing so-called “sensitive data”,
4. “There is no transfer [of data] to a third country..., where an individual in a Member State loads personal data onto an internet page which is stored on an internet site on which the page can be consulted and which is hosted by a natural or legal person who is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country”,
5. “The provisions of Directive 95/46 do not, in themselves, bring about a restriction which conflicts with the general principles of freedom of expression or other freedoms and rights ..”, while “it is for the national authorities and courts responsible for applying the national legislation implementing Directive 95/46 to ensure a fair balance between the rights and interests in question, including the fundamental rights protected by the Community legal order”.
6. “Measures taken by the Member States to ensure the protection of personal data must be consistent both with the provisions of Directive 95/46 and with its objective of maintaining a balance between freedom of movement of personal data and the protection of private life. However, nothing prevents a Member State from extending the scope of the national legislation implementing the provisions of Directive 95/46 to areas not included in the scope thereof provided that no other provision of Community law precludes it”.

On the grounds of those principles the Swedish Court is now called to decide the claim filed by Ms. L....

RFID technology and Biometrics: High potential, but also big trouble for marketers!

Marketers, distributors and retailers are more and more fascinated by the – unquestionable - potential offered by tracking technology. Fairly obvious are the advantages to be achieved through the use of such technology: constant monitoring of stock available and products running short, control on product’s location, effective countermeasure against shoplifting, consistent cost savings (linked to employees’ salary, human errors, delivery faults, etc.), quick self-checkout.

In addition research on consumers’ shopping habits, their monitoring and profiling will result both significantly more accurate and far easier to perform.

As to the technical aspects “giants” as IBM, INTEL, MICROSOFT, SAP and others are involved, a fact which eloquently testifies of the economical interests at stake and of the future potential assigned to the particular technology.

On the other side, privacy watchdogs feel clearly uncomfortable with the perspective of having people constantly traced in their daily moving (e.g. through chips inserted in their clothes) or located on work as well as in their private homes (through tags inserted into products’ packaging). Disclosure of consumers’ addresses would easily be implied by the use of RFID technology.

The discussion between interested business sectors and privacy watchdogs is heating up and both sides try to high lighten the pros and cons from their respective standpoints. While specific solutions and applications, as so-called “passive” chips (i.e. those not equipped with an energy source and therefore delivering signals perceivable by

monitoring PCs only within a certain distance from the controller's location) are proposed as a viable compromise, it could result useful to find out what's already going on with respect to RFID technology.

Germany/Italy/United States/United Kingdom:

UK

(1) During year 2003 in the UK (in a Cambridge shop) T....., one of the leading companies in the retailing sector, decided to start testing the effectiveness of tracking chips inserted in the packaging of a specific product (razor blades). At the moment the product was removed from the in-store shelf the chip switched a CCTV camera on, while a second picture was taken at the checkpoint.

Unfortunately this test procedure – even if clearly performed for security reasons - became public and steered angry reactions from shoppers who felt they were being targeted with an unacceptable privacy invasion. Protest actions were organized outside the retailer company's stores and the razor blade producer was asked to remove the chips form its packages. A representative of a civil rights group expressed concern about potential "function creep" (i.e. collection of information for a specific purpose being used for a different one). The retailing company rushed to declare that "We have not nor have we any intention of using this technology to track, videotape or photograph consumers" and to stress the importance of RFID for solving perennial business problems such as shoplifting, inventory shortages and logistical errors.

Italy/US

Identical problems - with respect to the use of RFID – hit B... Group, a well known Italian clothing producer, after announcing the company's interest in the new technology and proudly stating – in a common press release with the tag provider – that the particular device would result "imperceptible to the wearer and remain in individual items of clothing throughout their lifetime".

When press reports assumed that the company had started to embed tracking chips in its clothing products, advocates from the US privacy group CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) invited consumers to adopt a boycott on a worldwide basis (120 countries where B..... has a presence) against the company's products and warned that the chips could be used for more than just unwanted advertising, being able to link customers' data as name, credit card information to the serial number of the product and to track the "identified" subject any time he approaches a tag reader device

Rather surprised by such – apparently unexpected – opposition, B.....performed in a sort of U-turn and explained that the company, "always a leader in technological innovation in the clothing sector, is currently analyzing RFID (Radio Frequency Identification) technology to evaluate its technical characteristics and emphasizes that no feasibility studies have yet been undertaken with a view to the possible industrial introduction of this technology".

Interestingly, another renowned Italian cloth producer, using RFID technology in its Manhattan shop since 2002, did not run into trouble and got away with it.

Germany

German retailer M... (operating more than 2.000 stores throughout Asia and Europe) requested its top suppliers to insert special microchips into products' packaging. According to the company's plans the system's testing should start in 2004 (possibly in November) at 250 supermarket and wholesale stores in Germany. RFID technology is supposed to allow systematic tracking of merchandise by delivering – through the use of microchips and radio frequency signals transmitted by antennae to a computer – a constant information flow on its location.

By year 2007/2008 all of the company's German retailers (about 800 stores) are supposed to have passed on to such technology. In the meantime (i.e. in year 2003) a 9 months test run was performed in one German shop, selling groceries and household items, while in another store RFID tags are on test use – for self-checkout lanes and antitheft systems - on the products of a particular brand of women's apparel.

Canada/United States

(a) Earlier this year (in January) Canadian Press reported that the local branch of a well known US fast food company had introduced thumb and handprint scanners, connected to the Payroll Department, in order to control the employees in a number of its restaurants located in Winnipeg (where – differently from other Canadian Provincial legislations – workers enjoy less privacy protection as to working place monitoring).

While a top executive of the provincial ombudsman's office expressed the view that the practice raised serious concerns (particularly with respect to the collected data's use, especially those electronically stored), a spokesman of the company explained that:

- employees had not made complaints about the “time clock alternative”,
- strict control on data's use only for stated purposes was granted,
- workers had been explicitly informed about the company's privacy policy, a privacy manger had been hired in order to supervise the new system and its application, and, finally, that
- the whole procedure was still in a testing stadium.

(b) It's definitely not a secret that company W... , one of the leading retailers in the US, gathered its top 100 suppliers/manufacturers in a meeting, held in June 2003, in order to informed them that it:

- would require them to broadly use RFID technology on cartons and pallets received by its stores,
- would expect them to comply with such practice no later than by the end of year 2004 (2005 as to all other suppliers).

According to a report issued by consulting firm A.T. Kearney, RFID technology.

- would cut down costs for store inventory by 5% and those for labor force dedicated to warehouse inventory management by 7,5%, but also
- would imply for major retailers additional investments in the range of approx. 100.000 USD at each store for the new equipment required for data collection and management.

After an initially quite rushing approach, the US company, faced with huge concern and protest by privacy advocacy groups, seems now willing to consider a smoother initial rollout and a testing phase involving a limited number of stores and product categories.

However those trends will develop in the future, it's fairly obvious that companies intending to target the European market, when using such technology, will have to deserve utmost attention to the problems they're likely to face in the territories of member states of the EU.

Transferring simply well established domestic marketing practices to the EU is all but a smart move, at least as long as on the other side of the Atlantic Ocean violation of provisions set for purposes of personal data protection may result in a criminal ffence.

Felix Hofer is a leading professional in the area of marketing law in Italy. Felix is the member for Italy of the Global Advertising Lawyers Alliance (GALA). GALA is an alliance of attorneys throughout the world with expertise and experience in the fields of advertising, marketing and promotion law. Among the services GALA is able to provide is a "one stop shop" to individuals and corporations interested in the answers to questions and solutions to problems involving the complex legal issues affecting global advertisers and marketers. For more information on GALA and its membership, please visit www.gala-marketlaw.com or contact Stacy Bess, GALA's Executive Director at sbess@gala-marketlaw.com.