



GLOBAL ADVERTISING LAWYERS ALLIANCE

“ IT Meets Telecom “
CLA European Conference:
Munich, Germany
November 13-14, 2003

EVOLVING ISSUES IN THE INTERNET

“Liability of IPs, protection of personal data and free speech in an evolving internet environment.”

By:

Avv. Felix Hofer

Hofer Lösch Torricelli - www.hltlaw.it

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

One can best address this topic by viewing it as a Super Bowl game.

The teams admitted to the finals are vast, they are:

(a) Pressure Groups, (b) Public Authorities, Politic Entities, Regulators, (c) Providers, (d) Users, each of them pursuing different and mostly clashing/conflicting aims, to be identified as follows:

- with respect to the “ Pressure Groups “ (a):

- lobbying for industry or business (economic) interests
- advocating in favour of widely recognized principles (freedom of speech, no barriers to information, pluralism, cultural exchange, etc.)

- with respect to the “Public Authorities, Politic Entities, Regulators “ (b):

- providing some kind of viable legal framework for international relations
- meeting needs of common/general interests (safety, crime prevention, intelligence, preventive control, etc)
- granting adequate protection to sector groups/interests (consumers, children and minors, etc.)

- with respect to the “ Providers “(c):

- delivering services characterized by sophisticated (and rapidly evolving) technology,
- moving in areas where traditional “rules” and existing legal framework often result widely inadequate for dealing with the arising new issues/problems,

- facing interference and reactions from all the other players on the ground (a, b, d), mostly lacking of a sufficient level of the technical aspects involved by the questions at stake
- with respect to the “Users “ (d):
 - being targeted from all the other players mentioned above,
 - feeling at the same time attracted by the potential of new technologies (e.g. SMS, MMS, VOIP, etc) and “invaded” by their practical application (spamming, electronic marketing/advertising on cell phones, pop up ads, banners, profiling through RFID, fidelity cards, cookies, monitoring through audio-visual means, etc.).

Now the players, who are they?

- as to the “Pressure Groups “ (a):
 - Conglomerates and multinational companies,
 - Industry associations,
 - Sector groups (cultural, political, religious, etc.)
- as to the “Public Authorities, Politic Entities, Regulators “ (b):
 - The European Union (issuing directives and regulations)
 - National States and Authorities,
 - Independent Authorities (e.g. Data Protection/Privacy Commissioners and their trans-national body, i.e. the Working Party- DPWP)
- as to the “Providers “(c):
 - Their national association,
 - Their international associations,
 - Single companies (sometimes having a global structure or coverage)
- as to the “Users “
 - Consumer associations (national ones as well as international ones),
 - Other groups invested with the representation of specific interests

So, that’s the scenario of the game. Let’s now have a closer look at the strategies, the touchdowns and the fouls!

When talking about this subject we must not also forget the *Coaches* (legal experts) and the *Referees* (the Judges), which have at least one characteristic in common with most of the players on the ground (or most of them): a deep “ignorance” (i.e. “lack of knowledge”) about the technical aspects of the electronic means, they’re called to deal with. Therefore they clearly struggle when required to provide solutions for totally new problems and when trying to apply their proven expertise to new tools and mechanism.

The result:

- comprehensive discussions on issues as the “legal” nature of a website (could it be considered as a “newsstand” or rather as a “publishing house?”),

- headache favouring searches for legal provisions to be invoked for resolving disputes concerning such new technical means,
- desperate tries to come across situations, where the players are located everywhere and target everyone, where jurisdiction and enforcement problems frequently arise and result as riddles without solution.

Why are data protection and provider liability so relevant in the scenario of the Internet environment?

The answer to this question is always the same - linked to every service or activity performed within the area of electronic communication: **MARKETING**

Marketing – just as a broad range of other services present in Electronic Communication – 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 Centres, Research Companies), which subsequently involves specific liabilities for those subjects

Is the issue actually relevant? And how does it become so?

Data Protection Commissioners (i.e. national, independent Authorities, in charge of the Directive’s domestic implementation) tend to focus their attention more and more on new techniques, means and services, as:

- SMS,
- E-Mail or Electronic Ads (e.g. Pop up Ads),
- Cookies or "web bugs" (mini bits of code left on user's PCs),
- Banners,
- Java Scripts, Spy Ware (Keylogging)
- RFID (radio frequency identification) tags inserted in packaging, loyalty cards, smart shopping trolleys, clothes,
- Monitoring (low-level radiation cameras to “see” through clothing, walls or cars)

DP Commissioners:

- coordinate on a trans-national level (Data Protection Working Party - DPWP),
- concentrate not only on subjects established in the EU,
- try to extend control on foreign subjects using, while processing personal data, equipment located in the EU’s territory,
- claim for special codes of conduct (data processing on the Net, data recording through audio-visual systems, data use in Direct Marketing),
- do apply sanctions (fines, but violations of privacy rules can/may result relevant also as criminal offences, punished with imprisonment up to 3 years)

What can happen, what may turn out wrong?

Germany:

Earlier this year the court of Berlin (Landgericht – LG) was called to deal with a complaint about 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 defence 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 defence 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 behaviour (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) "RFID technology: a boomerang trial"

Very recently in the UK (in a Cambridge shop) 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 from 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.

(2) 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. The decision also contains useful indications as to identification of marketing communication.

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 defence's argument that a mailing list of subjects willing to receive promotional e-mails had been used was not considered as relevant.

United States/Italy:

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 analysing 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.

The D(ata)P(rotection)W(orking)P(arty), in its opinion of May 30th, 2002 issued some interesting indications as to the application of EU rules on privacy to data processing by web sites, based outside the EU and as to protection offered to individuals not being EU citizen

According to this opinion, the EU Directive no. 95/46/ (Article 4) states that national law becomes applicable:

- when data processing is carried out by an establishment's activity based within the territory of a Member State (if more countries are involved, compliance with all national laws will be required),
- if a data controller (not established on Community's territory) makes use of equipment, automated or otherwise, situated on the territory (unless use only for transit purposes, i.e. back bones, cables, etc. of telecommunications networks).

Where, for companies providing services via Internet as place of establishment will be considered:

- neither the place of location of supporting technology,
- nor the place at which web site is accessible,
- but the place where activity is pursued (e.g. a DM company registered in London, developing European wide campaigns there and using web servers located in Berlin and Paris; place of establishment would be London).

While, in the DPWP's reading, as disposal - not be confused with property or ownership – of technical equipment has to be intended that:

- not ANY interaction between an EU Net user and a web site based outside the EU implies application of Privacy Directive,
- to this purpose the relevant aspect may be found in the fact that the equipment is at controller's disposal for processing of personal data,
- as to the extent of disposal not full control on equipment is necessary, but a sufficient degree of disposal occurs, if data controller, in determining the way that the equipment works, makes relevant decisions as to data processing's procedure (e.g. choice of the data to be collected, stored, transferred, altered etc., in which way and for which purposes).

With respect to:

Cookies (standard part of HTTP traffic), containing any kind of info about targeted individual (e.g. pages viewed, ads clicked, user ID, etc.), the DPWP:

- considers conditions of data collection through cookies on a HD relevant for determining the law applicable,
- recommends:
 - o proper notice to the user about info stored, purpose, validity period (before cookies' placement)
 - o option for acceptance, rejection or choice on info to be released by subject targeted through cookies.

Java Scripts (i.e. software applications sent by web site to a computer),

- allowing remote servers to run applications on a user's PC.
- apt to be used for:
 - o collection and processing personal data stored in user's PC,
 - o providing customer with most „adequate“ banner or ad,
 - o subsequently for “profiling” (without user's awareness),

the DPWP considers such technology as a form of invisible and not legitimate processing

Spy wares (i.e. pieces of software secretly installed in PCs, e.g. when downloading other software, as music player),

- sending back personal information related to the data subject (e.g. music titles), and
- also known also as “ E.T. applications “, because (once lodged in user's PC) they “phone home” and report about data subjects habits, collect data and send it to another location,

the DPWP again considers such technology as a form of invisible and not legitimate processing

A heavily debated topic over the last few years has been Provider's liability. Why is Provider's liability such a controversial argument? The answer is simple: when it comes to unfair practices performed on the Internet all the players on the ground (legislators and regulating authorities, pressure groups, competing interests, targeted end-users) are faced with the following problem: how do I get the bad guys, how can I enforce legal provisions or judicial decisions against them?

Up till now nobody has been able to come up with a truly satisfying solution, even if everybody is convinced that there is a strong need for achieving one. So, the temptation of choosing to proceed on the easiest track is really huge. The Providers can be located, reached and caught. Usually they're

also strong enough - under a financial perspective - to result as appealing targets for lawsuits. That's – in my modest view – one of the main reasons why provider's liability has become such a popular topic and why they're easily put “*between the hammer and the anvil*”.

What's next? Despite a widespread call for a legal framework to be applied to the Internet, politicians and legislators have become more and more aware of the difficulties that have to be faced when trying to set up harmonized, strict and enforceable rules for a system inspired by a strong feeling versus freedom of information and widely appreciated just for such characterization.

Well aware of this aspect, recently (in Strasbourg, on June 28th, 2003) the Committee of Ministers of the European Union issued the “Declaration on freedom of communication on the Internet”, recommending that:

- the Internet should not become subject to restrictions, which go further than those, applied to other means of content delivery (Article 1),
- self-regulation or co-regulation should be widely encouraged for ruling content dissemination on the Internet (Article 2),
- in principle (and save achievement of goals of public interest as protection of minors), public authorities should not, through general blocking or filtering measures, deny access by the public to information and other communication on the Internet, regardless of frontiers (Article 3),
- existing barriers for accessing Internet communication and information services should be removed (Article 4),
- freedom should be granted as to providing services via the Internet (Article 5),
- no general obligation should be imposed on service providers as to monitoring of the content, which they give access to or they transmit or store; neither should service providers be held liable for content on the Internet when their function is limited to transmitting information or providing access to the Internet, while co-responsibility may hit them where they do not act expeditiously to remove or disable access to information or services as soon as they become aware of their illegal nature (Article 6) or, in the event of a claim for damages, of facts or circumstances revealing the illegality of the activity or information.
- for enhancing the free expression of information and ideas, the will of users of the Internet not to disclose their identity should be respected as long no responsibility for criminal acts is involved (Article 7).

Is everything OK for providers? A worrying and embarrassing past seems definitely over for ISP's; think about cases as: Hit Bit Software GmbH v. AOL, 2000 Germany - Godfrey v. Demon Internet Ltd, 1999 UK - Novell Inc. v. Renaat, C., 1999 Belgium - APRA v. Telstra, 1997 Australia).

Did the widespread protest against strong control on the Internet combined with the huge lobbying efforts and opposition from the subjects reluctant to take such an uncomfortable role in the play, succeed in easing the pressure on providers? Let's have a look around and find out what concrete experience reveals.

United States:

During the past summer (on August 13th, 2003) the U.S. Court of Appeals for the 9th Circuit handed down an interesting decision on provider liability. The case dealt with by the court involved a dating site and its operator and originated from the fact that a fabricated profile of an L.A. based actress contained real data (as name and address) combined with falsehoods. The operator got involved because of the interactive nature of the questionnaire generating the posting.

The Court of appeals held that Section 230 of the Communications Decency Act – CDA – had to be interpreted as follows: "So long as a third party willingly provides the essential published content, the interactive computer service receives full immunity regardless of the specific editing or selection process".

Germany:

Another area where provider liability may arise is domain name registration. In this context a German court (Oberlandgericht – OLG) in Hamburg recently rendered an interesting decision.

Two companies active in the foodstuff sector (sweets), one as the trademark owner, the other as the distributor of the products, sued an ISP, in charge of the assignment service of domain names and respective IP address numbers for alleged undue registration, in favour of third party, of an Internet domain corresponding to its trademark (“nimm2 - take2”). Such domain resulted to be linked to a Malaysian company

Previously a WIPO arbitration had decided for re-assignment of the domain name in favour of the German company owning the trademark.

Now the German companies (at this stage primarily seeking for recovery of legal costs) sued the ISP assuming that assigning the domain to the foreign company had performed a clear violation –under article 14/2, no. 3 - of the Trade Mark Act. In his defence the ISP argued that the enormous number of applications filed made it objectively impossible for the provider to perform a case-by-case check as to potential violations. Therefore such kind of control could not be reasonably expected from the ISP.

In its decision (dated February 27th, 2003) the Court accepted the defendant’s argument, holding that no co-liability could be found in the ISP’s service and therefore dismissed the claim.

So far, so good, but not all what shines is made of gold!

India:

In India a new regulation is coming up, meant to put onto ISPs the burden of proving their innocence with respect to connection’s misuse by service customers. According to Mumbai Police Department such regulation.

- access to Internet surfing should take place only to majors submitting a copy of their ID card,

- cyber libraries would set up,
- filtering software should be placed at the users' end,
- information should be stored for a certain minimum period and call-station identity should be recorded

Italy (and other EU member states?):

A crucial moment for the issue at stake will result the implementation of EU-Directive no. 2000/31 (on E-commerce).

Italy performed such implementation through Legislative Decree no. 70 dated April 9th, 2003, which deals in depth with provider liability, establishing the following criteria:

- Article 17 sets a general principle according to which a provider does not bear a general obligation of controlling the information transmitted or memorized; neither he's called to investigate actively facts or circumstances indicating illegal acts; on the contrary he's required to report such illegal acts, when acknowledged, to the competent authorities; finally – if request ed by authorities - he has to comply with instructions for immediate access blocking to illegal content,
- Article 14 affirms an identical exemption of content control and of liability with respect to “mere conduit” providers, save the following cases: (i) when the transmission of the message originates from the provider itself (??? As far as I can see, any electronic messages originates from a provider!), (ii) when the provider selects the receiver of the message, (iii) when the provider selects or modifies the information transmitted,
- Article 15, provides the same exemption for automatic, intermediate or temporary memorizing (caching) as long as the provider does not modify the information's content, complies with terms and conditions for access and updating of the information, does not interfere with the client's use of technology for profiling or data collection purposes, promptly removes the information once it's no more present in its original location,
- Article 16 allows such exemption also for permanent or long term information storage as hosting services performed by a third party (therefore housing clearly does not benefit from such provision), save the case in which the provider is aware of illegal acts conducted or illegal information supplied by its clients and does not remove promptly such content or block access to it.

Finally we do have exemption from provider liability! Nevertheless one cannot help asking themselves “where is the value added of such a masterpiece of legal regulation? Didn't a couple of articles in the existing Criminal Code and the general provision on tort liability in the Civil Code already cover all this?” I guess, definitely yes! But why complain as lawyers are offered a brand new battlefield for drawing clever litigation strategies and defence tactics? At least one business is for sure going to benefit from the new legal framework.

Felix Hofer

Hofer Lösch Torricelli

Via Delle Mantellate, no. 9
50129 - Florence
Italy



GLOBAL ADVERTISING LAWYERS ALLIANCE

Areas of Expertise

- Advertising, marketing and sales promotion law
- Administrative law
- Data protection and privacy issues
- Electronic commerce, intellectual property rights
- EU regulations.



Mr. Hofer, Dr. jur. Avv., is a founding partner of Hofer Lösch Torricelli, which provides legal services in throughout Italy, to Italian and foreign clients whose businesses require legal assistance either under the European, national or local regulations. His practice concentrates on counselling and litigation in advertising, marketing and sales promotion law, commercial, company and administrative law, data protection and privacy issues, electronic commerce, intellectual property rights, ecology and environment.

Mr. Hofer is author or co-author of a number of books and articles on advertising, marketing and sales promotion issues and on company law as well as a frequent speaker in congresses and seminars on related topics. He is the member for Italy of the European Advertising Lawyers' Association for which he served as the General Manager during the period 2001-2002 and of the Global Advertising Lawyers' Alliance.

Contact details

Email: fhofer@hltlaw.it
Telephone: +39 (0) 55 47 18 82
Fax: +39 (0) 55 48 60 86
Mobile: +39 33 55 61 10 93
Home: +39 (0) 55 60 69 84
Website: www.hltlaw.it



GLOBAL ADVERTISING LAWYERS ALLIANCE

Welcome to GALA, the Global Advertising Lawyers Alliance. The Global Advertising Lawyers Alliance is an alliance of lawyers located throughout the world with expertise and experience in advertising, marketing and promotion law.

The Global Advertising Lawyers Alliance provides a worldwide resource to individuals and corporations interested in answers to questions and solutions to problems involving the complex legal issues affecting advertisers and marketers.

Among the services GALA is able to offer its clients, is access to experienced practitioners of advertising, marketing, intellectual property, entertainment and promotion law and “one stop” international marketing clearance advice. With GALA on their side, clients can be assured that marketing material in all categories from radio, TV and print to the Internet - conforms to legal requirements, as well as clearance of international activities within the intellectual property and entertainment endeavors. E.g. International artists may clear a license or contract in various countries with an anchor member that would coordinate all services for all jurisdictions.

To contact experienced legal counsel in a particular country, simply visit the GALA website at www.gala-marketlaw.com and click on that country's name or flag.

