BEEP SCIENCE

SEMINAR:

Implementing Digital Rights Management on mobile devices

Speaker: Anne-Marie Pecoraro, Attorney at Law, Specialised in intellectual property
Head of the IPHT department and partner at Bignon Lebray & Associes
Chair of the Meritas IP working group (www.meritas.org)

CONTENT OWNERS SECURITY REQUIREMENTS

July 7, 2005, LONDON

BIGNON LEBRAY & ASSOCIÉS

Société Civile Professionnelle d'Avocats

14, rue Pergolèse
75116 Paris, France

Tél : (33) 01.44.17.17.44
Fax : (33) 01.44.17.98.99

e-mail : apecoraro@bignonlebray.com

CONTENT OWNER SECURITY REQUIREMENT

In January, Bignon Lebray & Associés had the pleasure of being invited, within the context of MIDEM 2005, to co-chair a workshop on the Entertainment Mobile Market

(http://www.bignonlebray.com/departements/pint/article.php3?id_article=322)

Our reflection is now carried a little further with respect to the characteristics of this new fascinating market given that our intervention today is specifically dedicated to the issue of content security requirements in the context of their use by mobile phones.

Since the consecration of Digital Rights Management in the law (not yet implemented in France in June 2005), the concept of content protection has evolved rapidly.

This issue is all the more important in emerging markets such as China, a nation where counterfeiting is rampant. The mobile market seems

particularly appealing, for it offers better ways of controlling such operations and makes the fight against counterfeiting more efficient and realistic.

At the legal level, we will have the pleasure of making a presentation on this topic on July 7 in London, at the Mobile DRM Conference which is organized by Beep Science (www.beepscience.com) on the following issues:

I – How do content owners set security and IPR protection requirements : (Digital Content Distribution and Intellectual Property Rights (IPR))?

II – How will security requirements affect mobile handset manufacturers ?

III – Liabilities when a handset is hacked ; who is responsible?

I – HOW DO CONTENT OWNERS SET SECURITY AND IPR PROTECTION REQUIREMENTS : (DIGITAL CONTENT DISTRIBUTION AND INTELLECTUAL PROPERTY RIGHTS (IPR))

Upon which regulation will the content owners rely to ensure the protection of the works, through the DRM in the European Community?

Faced with piracy, what are the solutions which have been developed by normative texts in order to fight against it? Actually, two means of prevention against piracy have been developed in the different Western countries: the system of collection from digital supports and devices (as we call it in France “private copy” which is a compensation paid on blank supports for private copies) and the optimisation of digital rights management systems (DRM).

The technology related to digital rights management and technological protection measures seems to be the best fit for guaranteeing creators reasonable remuneration in consideration of their works and for allowing European consumers to fully benefit from digital contents.

The DRM is a management system which may be defined as the association of management and software technology for copyright protection designed to control the sale and broadcasting of works or digital and multimedia contents. This system would allow, in particular, to guarantee that only users who have paid for their access to content actually have access thereto. The DRM is operated together with TPM (technological protection measures) which re-groups technology allowing companies of music or video content to secure and protect such content against any non authorised uses.

Faced with a topic consisting of the « legal protection of DRM in the EU », we found it relevant to focus on the major European event in that respect, namely Directive 2001/29 dated May 22, 2001 with respect to the harmonisation of certain copyrights and neighbouring rights within the information society. From all of the contributions of this Directive, we have decided to focus our attention on the main tools implemented by law in order to establish DRM systems, that is to say both the obligations related to technological measures and those related to information with respect to rights management. As a matter of fact, granting protection to TPM results in the reinforcement of DRM. Let’s analyse the methods whereby European law has dealt with the issue in relation to digital rights management.

We shall therefore first identify the TPM tool, at the service of DRM (Part I). Next, we shall acknowledge the recognisance of their protection by Directive 2001/29 (Part II), as well as the scope thereof (Part III and IV). Lastly, we shall analyse the impact that the said evolution may have on licensing. (Part V). The issues are Important notably in respect to legal aspects of intellectual property rights and digital distribution into cross media platforms.

Part I: Technological and information measures - The tools at the service of DRM?

A number of countries have signed two treaties regarding the establishment of global anti-circumvention laws – the Wipo Copyright Treaty and the Wipo Performances and Phonograms Treaty. Some countries have passed laws implementing these Wipo Treaties, the most notorious example being the Digital Millennium Copyright Act in the United States.

Under the terms of our Directive, technological measures are related both to information with respect to copyrights management and to the

protection of works, as regards the access and the use of such works (those protected measures are central component of DRM systems). However, we may wonder whether these measures effectively result in rights being duly respected.

1 Types of protection measures

The European Directive dated May 22, 2001 relating to the harmonisation of certain aspects of copyrights and neighbouring rights within the information society provides for two types of technological measures.

(i) Technological identification measures

The main purpose of technological identification measures is to serve as a support to the insert of data relating to a given work, so as to identify it, whether with respect to the title of such work, the author's and right holder's identities and the terms and conditions of utilisation. In other words, such data is constituted by information in relation to rights management pursuant to article 7.2 of the aforementioned Directive related to « copyrights ».

Various types of technology may fulfil such identification function, and may also directly protect copyrights, either by providing a protection function against copying, by means of a visible marking, thus limiting the risks of illegal use, or by guaranteeing the integrity of a work.

(ii) Technological protection measures

Article 6.3 of the Directive provides a wide definition of technological protection measures, which consist in any means, regardless of its mode of transmission (through network or support) or physical location (on the created work or on the recorded support), which hinders or restricts infringement of copyrights, neighbouring rights or *sui generis* rights of a database.

Devices, components or technologies resulting in restricting acts, which have not been authorised by right holders are therefore those concerned. They include both the technological measures which prevent one from accomplishing acts falling within the authors' legal monopoly and the technological measures which prohibit uses denied by right holders.

However, the Directive, as the WIPO Treaty, requires that technological measures be effective. These measures *« shall be deemed « effective » where the use of a protected work or other subject-matter is controlled by the right holders through application of an access control or protection process, such as encryption, scrambling or other transformation of the*

work or other subject matter or a copy control mechanism, which achieves the protection objective ».

Technological protection measures are usually divided into two categories:

- **Technological measures allowing access to works**

This category of technological measures prevents a non-authorised person from accessing a work protected by copyrights. The purpose thereof is to adjust or prohibit the access to the creation.
This control is assured either in an active manner by an identification process, by using an access code or an identifier, or in a passive manner, by using a decoder.

Quite a number of technologies protecting access rely on an encryption mechanism. Encryption consists of jamming contents, which prevents their use without decryption by means of an appropriate key, the said key being provided only to authorised users and/or authorised products.

- **Technological measures controlling the use of works**

Technological measures which control the use of works are technological tools designed to prevent any acts subject to the beneficiaries' exclusive rights, such as transmission to the public, digital copies, etc. from being accomplished.

In the United States, technological protection measures against copying have been introduced into legislation under the form of the *Serial*

Copyright Management System (SCMS), which is part of the *Audio Home Recording Act* dated 1992.

2 Reality of technological measures

Technological measures only constitute purely technological means of protection designed to guarantee the security and respect of copyrights. Nonetheless, it has been proven necessary to reinforce such a dissuasive impact by means of legal protection.

Part II: Taking DRMs into account through the protection of technological and information measures

For the purpose of dealing with this issue, the European Union has carried on with the works of the WIPO Treaty dated December 20, 1996, in the Directive with respect to certain aspects of copyrights and neighbouring rights within the information society. This Directive is to be implemented by the end of 2002 (but it hasn't been yet in all European countries).

1 WIPO treaties dated December 1996

The WIPO Treaty dated December 20, 1996 provides for two types of protection in order to discourage any attempts of piracy, which results in reinforcing DRM.

(i) Protection of technological means

Article 18 of the Treaty provides that :

> *« Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by performers or producers of phonograms in connection with the exercise of their rights under this Treaty and that restrict acts, in respect of their performances or phonograms, which are not authorized by the performers or the producers of phonograms concerned or permitted by law ».*

Technological measures must therefore be efficient, they must be implemented by authors in connection with the exercise of their rights, and restrict acts which have not been authorised by the relevant authors or by the law.

(ii) Information Protection

Article 19 of the Treaty lays down the obligations related to information with respect to rights management. Such wording may be construed as « *information which identifies the performer, the performance of the performer, the producer of the phonogram, the phonogram, the owner of any right in the performance or phonogram, or information about the terms and conditions of use of the performance or phonogram, and any numbers or codes that represent such information ».* Therefore :

« 1) Contracting Parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty:

(i) to remove or alter any electronic rights management information without authority;

(ii) to distribute, import for distribution, broadcast, communicate or make available to the public, without authority, performances, copies of fixed performances or phonograms knowing that electronic rights management information has been removed or altered without authority ».

The two above mentioned types of protection are those stated in the European Directive, such Directive directly resulting from the WIPO Treaty.

2 Directive dated May 22, 2001

Articles 6, 7 and 8 of this Directive provide for a protection of both technological and information measures, accompanied with sanctions.

(i) Obligations related to technological measures

Article 6 provides that Member States must provide for appropriate legal protection against circumvention of technological protection measures, as well as against the preparatory acts to such circumvention (see below).

(ii) Obligations related to rights management information

Under article 7, rights management information means *« any information provided by right holders which identifies the work or other subject-matter referred to in this Directive or covered by the sui generis right provided for in Chapter III of Directive 96/9/EC, the author or any other right holder, or information about the terms and conditions of use of the work or other subject-matter, and any numbers or codes that represent such information ».* On the basis of the new text, Member States must now provide for an appropriate legal protection against any persons which knowingly carry out (the intentional nature of the act is taken into account), without any authorisation, one of the following acts:

a)« the removal or alteration of any electronic rights-management information,

(b) the distribution, importation for distribution, broadcasting, communication or making available to the public of works or other subject-matter protected under this Directive or under Chapter III of Directive 96/9/EC from which electronic rights-management information has been removed or altered without authority ».

(iii) Sanctions and remedies

Article 8 imposes the obligation upon Member States to provide for *« appropriate sanctions and remedies in respect of infringements of the*

rights and obligations set out in this Directive and shall take all the measures necessary to ensure that those sanctions and remedies are applied. The sanctions thus provided for shall be effective, proportionate and dissuasive. *And each Member State shall take the measures necessary to ensure that right holders whose interests are affected by an infringing activity carried out on its territory can bring an action for damages and/or apply for an injunction and, where appropriate, for the seizure of infringing material as well as of devices, products or components referred to in Article 6(2).* Lastly, *Member States shall ensure that right holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right »*. Member States must thus provide for *« effective, proportionate and dissuasive »* sanctions against those who affect copyrights. The sanctions provided for are the granting of damages and, where appropriate, the seizure of infringing material and of other devices, both as result of circumvention or preparatory acts. France is likely to opt for criminal sanctions, which shall not prevent the initiation of proceedings at the civil level at the same time. Reinforcing sanctions is also strongly required.

Europe has thus chosen to provide itself with a legal structure which shall sanction any persons who may act against the measures taken by music authors, in particular within the context of a DRM. However, its efficiency remains uncertain.

Part III: Efficient protection at the service of DRMs

A third level of protection has been established by the Directive. The first two levels are constituted on the one hand by the existence of the utilisation monopoly under the form of protected rights and on the other hand by technological measures as such. Its efficiency may be assessed by means of prohibited acts and commission monitoring.

1 Prohibited acts

The European Directive prohibits both circumvention in itself and preparatory acts to the circumvention of technological measures. Such dichotomy only relates to technological protection measures. With respect to information measures, only circumvention only prohibited.

(i) Circumvention

Protection against acts which affect information measures in relation to rights management consists in sanctioning circumvention (article 7§1 of the Directive). The modification of information, and in particular, its suppression are expressly concerned. Any acts which result in affecting information with respect to rights management are thereby sanctioned. Preparatory acts, the purpose of which is to circumvent information measures are not sanctioned in themselves.

As indicated previously, articles 7§1 (a) and (b) also prohibit any utilisation of the work or subject-matter, the information of which has been altered. Such illegal utilisation implies that information has been

previously affected, that is to say that the circumvention of the technological information measure has already occurred.

Under article 6 § 1,the Directive with respect to copyrights and the information society also prohibits the circumvention of technological protection measures.

« Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective ».

The fact that the person committed such circumvention with more or less knowledge of his or her fault, is a determining factor as regards to the qualification of circumvention : if such a person has deliberately circumvented a protection measure, or with reasonable grounds to believe that he or she was doing so.

(ii) Preparatory acts

Preparatory acts are acts accomplished prior to circumvention, whether or not such acts result in circumvention.

The prohibition of preparatory acts is stated in articles 6 § 2 of the Directive and constitutes one of the main contributions in comparison with the WIPO Treaty with respect to copyrights.

However, only preparatory acts to technological protection measures are concerned. Article 6§2 imposes the obligation upon Member States to provide for appropriate legal protection:

«against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:
(a) are promoted, advertised or marketed ***for the purpose of circumvention of****, or*
(b) have only a ***limited commercially significant purpose or use other*** *than to circumvent, or*
(c) are ***primarily*** *designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures ».*

Certain preparatory acts to circumvention do not fall within the scope of application of the protection of technological measures and are therefore not sanctioned.

Such is the case for the transmission of intellectual solutions, advice or instructions which result in circumvention. The publication of the source code of a technological protection measure would thus not be sanctioned, contrary to the system implemented by the Digital Copyright Act of 1998.

On the one hand, only preparatory acts, the sole or main purpose of which is the circumvention of technological measures are prohibited. It has indeed been considered as logical that industrialists that launch on the market products intended for legal purposes but which may

potentially be used for purposes of circumvention should not be sanctioned. It may raise issues in terms of interpretation by the courts. The Directive recommends moderation to Member States, by taking into account, in its whereas 48, industrialists' commercial interests.

The French Code of Intellectual Property does not contain any of these measures. The works in connection with the implementation of this Directive carried out by the *Conseil Supérieur de la Propriété Littéraire et Artistique (CSPLA)* will allow the verification of whether these rules have been implemented under ordinary law with respect to infringement, in the absence of creation of independent or specific rules. However, the issue remains at stake.

2 Protection strengthened by European Commission Monitoring Control

The European Commission ensures the monitoring and control of the Directive.

Pursuant to article 12 of such Directive, the Commission transmits to the Parliament, to the Council and Economic and Social Committee, a report which examines whether the level of protection of technological measures as required under article 6 is sufficient enough and whether this system does not contradict the acts authorised by the law. The Commission may present proposals with a view to modifications of the Directive for the purpose of ensuring the due functioning of the internal market.

Article 12 also provides for a contact committee *("comité de contact"),* the aim of which is « *to examine the impact of this Directive on the functioning of the internal market, and to highlight any difficulties; to organise consultations on all questions deriving from the application of this Directive; to facilitate the exchange of information on relevant developments in legislation and case-law, as well as relevant economic, social, cultural and technological developments; to act as a forum for the assessment of the digital market in works and other items, including private copying and the use of technological measures ».*

This protection is however limited.

Part IV: DRM faced with diverging interests

Firstly, a cooperation between right holders and industrialists is necessary (We will talk about this in the second part of this speech).
Secondly, users benefit from exceptions to copyrights.

Contradictions and divergences: the consumers' expectations

From a legal point of view, two systems of law are in conflict. On the one hand, the beneficiaries' perfectly legitimate right to protect their products against illegal copies, and on the other hand, the right to private copies that users will not fail to invoke, which is just as legitimate and established in the Directive.

Yet, technological protection measures are operated without establishing any distinction between legal and prohibited acts. The application of

these devices thus results in threatening the free exercise of exceptions to copyrights.

Exceptions to copyrights account for an essential part of literary and artistic property which may be justified by the necessity to ensure the balance between the beneficiaries and users' respective rights. It is mainly related either to practical grounds, as the impossibility to ensure compliance with exclusive rights in the user's private sphere, or to fundamental rights and freedom.

The European Directive has thus incorporated in article 6 thereof, provisions designed to guarantee the exercise of exceptions by works users.

Member States must therefore take any appropriate measures in order to ensure that beneficiaries of exceptions or limitations, stated in a limitative way in articles 5.2 and 5.3 and which consist in reprography (art. 5.2 (a)), specific reproductions by libraries and archives (art. 5.2(c)), short-lived recordings by radio-broadcasting organisms (art. 5.2 (d)), reproductions by social non profit making institutions (art. 5.2 (e)), uses for illustration and teaching purposes (art. 5.3 (b)), uses for the benefit of disabled persons (art. 5.3 (b)), uses for public security purposes (art. 5.3 (e)), may benefit from any such exceptions or limitations.

Nevertheless, as regards to private copies, the State's intervention is not compulsory:

« A Member State may also take such measures in respect of a beneficiary of an exception or limitation provided for in accordance with Article 5(2)(b), unless reproduction for private use has already been made possible by rightholders to the extent necessary to benefit from the exception or limitation concerned and in accordance with the provisions of Article 5(2)(b) and (5), without preventing rightholders from adopting adequate measures regarding the number of reproductions in accordance with these provisions. »

The whereas 39 also seeks a fair balance, providing that the exceptions should not inhibit the use of technical measures or their enforcement against circumvention.

What will happen to the balance of interests if, for instance, it is not possible to get access to a piece of work that fell within public domain, or if there is no guaranty to the exercise of legal exceptions?

☆ **Contradictions and divergences: privacy issues**

Please recall that the application of DRM is likely to involve very specific consumer-related personal data, and that one of the main controversial issues in that regard is to ensure the protection of privacy.
For Instance, when a software is used by a distributor acting as an intermediary between content owners and media players, the operator-distributor has access to the names or alias of the users, their e-mail addresses, credit card numbers, etc…: then, the distributor must act as a trustworthy third party. However, it is possible to resort to a third party

authority, neutral and independent, in order to face the risks attached to the centralization.

Part V: Security and IPR protection requirements in licensing

The introduction process of DRM purposefully refers to the issue of the organization of collective management.

Before rapidly dealing with this subject, we shall raise a few questions on the way content owners, in this digital economy, consider the licences that they grant, (i.e. in the event of cross-platform distribution).

In this respect, let's emphasize the interest that such techniques, object of our reflection, represent in the context of the expansion of television on mobile phones, which was decidedly launched on the French market recently.

1 Negotiating agreements and standard terms with rights owners on clearing of rights as well as on technical legal aspects

(i) Provisions to protect the value of the content

Some content owners, such as subsidiaries of Major Companies, have organized their own mobile platform distribution.

Other content owners have entered into partnerships with companies such as Musiwave, whose part oversteps the one performed by the

service providers with regard to the organizational capacities that they offer.

The various geographical markets offer different potentials: in the North American market, operators tend to take on more responsibilities; in significant Asian markets, the different systems and protocols used, compared to European markets, give rise to technical curbs…

Most certainly, in any case, the content owners are in a position to require that provisions be incorporated in the standard terms to ensure and guaranty that their partners will maintain a certain level of security.

Concerning the agreements drafted by our firm, we are accustomed to request that any of the parties involved be able to justify the level of performance and security that they utilise. As an example, a producer shall be able to contractually require an 2.0 OMA / DRM version. A significant portion of the market operators that we know shall react in that sense and wish to submit their whole catalogue, at the best level standard.

This authorisation can be combined with a termination provision in relation with our subject : for example, breach and termination of licence, if the works or recordings are distributed through a DRM, whose standard is different from the authorised one, or if the distribution is compatible with mobile devices, which were blacklisted and excluded because they did not offer a satisfying security level.

Nevertheless, it is not impossible that some media companies might accept to use an OMA v1 DRM forward lock mechanism (encoding) for

some content (typically light media content that has lower value) and others that require higher security for e.g. full track music downloads - requiring encryption.

Currently, as long as it would concern a same group's catalogue exploitation, we have most often been confronted with homogeneous requirements. At a certain level of technical standard and for a type of given exploitation, the authorisation is granted or not.

DRM can also be very useful to implement temporal or geographical restrictions : for example, to allow downloading only in a given territory. In a decision of the French Competition Council on November 9, 2004, upon which we will comment hereafter, the competition authority has recalled that the Microsoft WMA allows the user to determine, for each type, the utilization restrictions, which will be linked with it. It also recalled that the Apple DRM, Fairplay, includes rights, which were determined once and for all (7 engravings, downloading on 3 computers).

Regarding the sector of paid downloading of music through the Internet, the French Council considered that the rigid determination of rights constituted a lack of flexibility, which could represent a disadvantage for the producers, which would prefer being entitled to choose, which rights will be associated with each title. This precision shows that a differentiated strategy (according to each type of catalogue) could potentially develop.

(ii) Invoicing models and pricing

* Financial issues for the content :

One of the crucial roles of the DRM is to allow the management and repartition of the right owners' remuneration, in exchange for their granting of use. This is why we found it interesting to illustrate our debate trough examples of remuneration sharing.

Some rights owners and service providers deem the share of the net price which may be received by the operators excessive..

The problem of "airtime" (the surfing/navigation time) is not clear : is it counted or not by operator for its invoicing during downloading or in the lump sum price ?

The difference will be dispatched among the authors, the producers (and the artists), and service providers.

Logically, the rights holders should claim a percentage of the end-consumer price (and not a share of the wholesale price like for records) as well as a minimum amount. As the tariff must result from negotiations and cannot be imposed, operators and service providers do not accept easily a minimum amount.

On one hand, with respect to ringtones or realtones, some deals have been clearly reached (the producers having mandated their collective management companies in France, and acting directly in others countries).

- For Sacem, 12% of the RP. With a minimum amount.

- For French producers, not a royalty, but a fixed price for a ring. A minimum amount (a few cents) depending upon the technical quality, and the length (for instance 30 sec.). (With MG).

On the other hand, with respect to listening or downloading musical contents, the agreements are still more experimental.

The French collective management society SPPF has negotiated a frame, with standard terms, allowing to its members to rely upon this negotiation. The standard terms are focused on music uses and not marketing terms.

Cross marketing, advertising investments, etc, have to be negotiated by the producers and should modify the royalty rates.

Regarding editors, copyrights owners and SACEM, the issue of minimum amount remains unclear : will they receive a minimum of 0,10 euros ? 0,25 euros ?Between 0,15 and 0,25 euros according to the sales price ? What will be the rule, in the case of consumption acts through SMS ? Or through a WAP link (possibly with a payment through SMS).

Controversial issues in the US:

- Some copyright holders wish to negotiate and deal only with the operators, not the labels;

- The issue is raised with respect to the qualification of certain exploitations under reproduction rights or mechanical rights.

- Synchronisation right: the application of a regime is likely to change the cost

2 The role of Collective management societies

To some extent, technological measures may restore the exclusivity of rights and well as their individual exercise by rights holders. Indeed, rights holders may now rely on technological means to impose compliance with their moral and patrimonial rights thanks to technological identification and protection measures.

However, in the digital age, the possibilities and needs generated by the information society seem to promote the development of their collective management.

DRM seems to be the obvious solution, since it guarantees an efficient management, with respect to the number and scope of uses authorised by the information society. As a matter of fact, technological information measures constitute genuine prospects as regards to rights management. Information with respect to rights management will necessarily lead to the electronic management of creations, the scope of which will develop in an exponential manner with distribution through digital networks.

The issue in relation to the collective rights management has not given rise to harmonisation at the European Community level yet. In spite of a communication, dated 1996 (following the Green Book *(« Livre Vert »),* which concluded upon *« the necessity to define, at the Community level (…) the rights and obligations of collective management companies*

(…) », the European Directive has not provided for the fully harmonised regulation of collective management. However, in its whereas 17, it considers that *« it is necessary, especially in the light of the requirements arising out of the digital environment, to ensure that collecting societies achieve a higher level of rationalisation and transparency with regard to compliance with competition rules ».*

Entering into agreements with authors' unions has become a necessity in the digital environment. Only greater coordinated and integrated rights management may simplify the organisation of rights management, which appears to be quite confused for the time being.

In France, various authors' unions have gathered within SESAM organisms in France, in charge of implementing a common and complete rights management. The French CSPLA has suggested establishing an information and orientation platform common to all collection and rights allocation companies, thus ensuring the identification, by means of a sole consultation, of the protected works or subject-matters registered with the authors' unions and which may be researched by users, as well as the right holders and the nature of the duties likely to be acquired from them.

The user shall be directed by electronic means to the right holders with whom they might acquire on-line rights. The delivery of digitized works by electronic means may also be contemplated.

The exploiting rights that are being granted by some collective management companies around the world, should provide for the requirement of a certain level of security on the technical level.

II – HOW WILL SECURITY REQUIREMENTS AFFECT MOBILE HANDSET MANUFACTURERS ?

In the European Community initial regulation texts, there are no constraints for the manufacturers regarding the DRM implementation of the mobile devices that they produce. Nevertheless, the market reality incites them strongly to take DRM into account. Moreover, mobile devices that do not offer a sufficient level of security can be blacklisted and excluded, in the licences granted by content owners. DRM implementation in mobile devices depends on cooperation and negotiation. Generally speaking, the organisation of the brand new sector of the digital entertainment market is a good context for cooperation and negotiation between the professionals of this sector, which will play important roles in the future (OMA, Mpeg La, Gsm Association MEF - mobile entertainment market, CMLA – Content Management License Administrator, collective management companies, consumers associations, in France: Geste…)

1 A necessary cooperation between right holders and industrialists

Some technological systems require an identifying signal from the playing, reproduction or downloading devices; protection is incorporated into the support or digital code of the work, which sends a signal to devices so as to prevent them from affecting copyrights (non-authorised access, work reproduction, etc.)

The establishment of efficient technological devices may only result from consultation and cooperation with equipment and support providers.

Yet, the Directive, in its whereas 48, like the the Digital Millennium Copyright Act, includes a clause referred to as “no mandate”, which does not impose any obligation upon industrialists to adapt their products to technological devices. The industrialists’ independency is therefore preserved. To that end, the Directive provides that:

« *Such legal protection should be provided in respect of technological measures that effectively restrict acts not authorised by the rightholders of any copyright, rights related to copyright or the sui generis right in databases* ***without, however, preventing the normal operation of electronic equipment and its technological development.*** *Such legal protection implies* ***no obligation to design devices, products, components or services to correspond to technological measures,*** *so long as such device, product, component or service does not otherwise* ***fall under the prohibition of Article 6.*** *Such legal protection should respect proportionality and should not prohibit* ***those devices*** *or activities which have a commercially significant purpose or use* ***other than to circumvent*** *the technical protection. In particular, this protection should not hinder research into cryptography ».*

If we establish a comparison with American Law, we notice that the DMCA provisions are similar :

No Mandate - Legislative History

1 <u>Statutory Provision (17 U.S.C. 1201(c)(3)):</u>

> (3) Nothing in this section shall require that the design of, or design and selection of parts and components for, a

> consumer electronics, telecommunications, or computing product provide for a response to any particular technological measure, so long as such part or component, or the product in which such part or component is integrated, does not otherwise fall within the prohibitions of subsection (a)(2) or (b)(1).

There are two rules: The first rule is that manufacturers are not legally constrained to adapt their devices to DRM, the second rule is that they are compelled, like anyone subject to justice, to comply with Article 6 of the Directive.

It is important to recall that under article 6 § 1, the Directive prohibits the circumvention of technological protection measures. The prohibition of preparatory acts is stated in articles 6 § 2, and only preparatory acts to technological protection measures are concerned. However, industrialists may claim the benefit thereof and invoke any such provisions only to the extent that they have not themselves affected the legal protection of technological measures.

The whereas 48 of the Directive encourages moderation and proportionality.

Cooperation between right holders and technological industry thus needs to be enhanced.

Accordingly, the efficiency of technological measures shall depend on the industry's good will to incorporate into equipments mechanisms which ensure the interaction with technological devices.

In fact mobile manufacturers should undertake on a volunteer basis to distribute only those digital files, including recordings, for which the relevant authorisations have been obtained.

It is of interest to quote in this regard the principle of the directive, according to which: *"Important progress has been made in the international standardisation of technical systems of identification for works and protected subject-matter in digital formats. In an increasingly networked environment, differences between technological measures could lead to an incompatibility of systems within the community. Compatibility and interoperability of the different systems should be encouraged. It would be highly desirable to encourage the development of global systems."*

By means of an example, the CMLA website mentions: *"The CMLA initiative, together with the Open Mobile Alliance's DRM 2.0 Enabler Release, addresses the burning market need for an open standard-based digital rights management platform the right way at the right time."... "Achieving cross-industry alignment on interoperability and implementation consistency issues is crucial to making innovative digital media services a reality. The common basis will considerably speed the multi-vendor introduction of interoperable media enabled products; from mobile devices and consumer electronics to PC media players..."*

2 Choosing a system and negotiating a price (patent licence)

The importance of the question of interoperability

The DRM system involves a chain of operations between :

- The encoder,
- the server,
- the terminal or player,
- the rights dispatcher.

But numerous systems of DRM exist, as well as a wide variety of terminals, players or mobile devices. Consequently, the problem of interoperability between the various systems is a crucial issue. The interoperability depends on a good cooperation between industrialists. The use of DRM on mobile phones also depends on an agreement on tariffs (for the use of patents, which protect DRM technologies).

As we know, (and this illustrates our debate) , a first offer to the mobile phone manufacturers resulted from the work of the Open Mobile Alliance and the MPEG Licensing Authority. This offer concerned tax rates for the utilisation and the implementation of DRM patents, which amounted to: US $1 per mobile unit (payable by the party that offers the device to an end user) and 1% of the transaction price (payable by the service provider). This royalty rate was offered in connection with products that have OMA DRM 1.0 functionality or OMA DRM 1.0 and OMA DRM 2.0 functionality.

This first offer having not been accepted, it was followed by a second offer, in spring 2005, which was also badly received, as the mobile

manufacturers considered that it was too expensive. Under the revised licence terms, royalties for the right to make and sell OMA devices will be US $0.65 per device (payable by the party that offers the device in hardware or software to an end user). This proposal is intended to cover a device combining both OMA DRM 1.0 and OMA DRM 2.0.

Royalties for each transaction employing OMA DRM 1.0 will be a flat US $0.25 per subscriber per year.

Mobile manufacturers have announced that, according to them, a high price would incite them to use less expensive technologies, and possibly even proprietary technologies. The price notably determines a strategy to choose or build their own DRM technology.

There is a danger for the market to fragmentise and no longer provide universality, efficiency and homogeneity of DRM technologies (compatible with each other). Nevertheless, one can consider that, generally speaking, tariff reduction will accelerate the OMA launching by manufacturers and mobile networks operators. This choice will be in their interest, as it will correspond to a rise of average revenue per user. The stimulation and the market's natural incentives, as it evolves, must incite mobile manufacturers to find DRM solutions that would be economically acceptable for them and, in any case, ensure the required security level.

Otherwise, (even without legal constraints on this matter), a mobile manufacturer who does not take into account security requirements, would run the risk of being marginalized. Notably, there is a risk for its devices to be blacklisted and contractually rejected by content owners.

For example, during the last Midem symposium in 2005, the worldwide director of a major mobile manufacturer declared : “In the past, we’ve just made the delivery device and left it to the operators to solve the consumers’ needs. Now we work with operators and adapt products to their requirements. At the same time, we bring to them some ideas that they can incorporate, so it isn’t a one-day communication.”

If we establish a comparison with the PC market, we can realistically believe thatPCs and consumer devices will probably come embedded with hardware-backed DRM and other policy controls by the latter half of 2005.

3 An example in France of competition issues

As we know, OMA DRM 2.0 is more complex because it is intended to apply to devices with more capabilities and more security features. OMA DRM 1.0 was designed to support ring tones and wallpaper graphics, in the framework of simple, low-cost devices with not much memory, no trusted system clocks, and no sophisticated content rendering capabilities. OMA DRM 2.0, in contrast, is designed for more powerful devices that have the ability to play higher-resolution audio (such as actual music tracks) and video, send content to other devices and store data. At the present time, it is unclear how the ability to copy content to other devices that a person owns will affect the choices and liabilities of the implementers.

The interoperability problem leads to competition issues and competition law implementation dilemmas. ITunes is the only digital music store that the iPod supports (although it can also play unprotected MP3 files).

Additionally, Apple has integrated the exclusive use of iTunes in its ITMS utilization conditions, the use of another software being forbidden. These are the elements of a thrilling case, which was judged by the French Competition Council on November, 9th, 2004, in the sector of music downloading on the Internet and numeric mobile music devices. This decision should really be commented upon, even though it was dedicated to the data downloading on the Internet and not to mobile phone exploitation, as it describes the market and provides relevant elements for an analysis of what will happen in the future.

The Competition Council, (which in France has the authority to judge infringements to competition law) has analysed the French market. It determined that the market for paid online music downloading in France is shared by six major companies : FNAC, Virgin Mega, OD 2, Sony Connect, E-Compil and iTunes Music Store.

Regarding the encoding and DRM devices, the paying platforms use the following couples :

Apple's platform, ITunes Music Store uses the AAC/Fairplay couple ; Sony's platform uses the Atrac/Open MG couple ; all other paying French platforms use the WMA/ Microsoft's DRM couple. Virgin Mega, subsidiary of the Lagardère group and sister company of Virgin Mégastore brought a complaint against Apple before the Competition Council, because Apple refused to grant any licence over its DRM Fairplay software. The consequence of this licence's refusal is that the tracks downloaded on the virginméga.fr website can not be listened to on an iPod.So Virgin Mega pleaded before the Competition Council that the DRM access Fairplay was necessary for its activity of online music

operations and that, because this software DRM was an essential resource, Apple's access refusal constituted an abuse.

Virgin Méga mentioned the previous cases on matters of competition law concerning the notion of "essential facility". This means that, under specific conditions, an operator that owns an essential facility for other operators can be legally forced to grant a licence. This decision needs to be commented on in the framework of our debate on DRM exploited for mobile phones. Indeed, the Competition Council has not accepted the claim of Virgin Mega, which demanded a licence to be ordered regarding the DRM software, under economically equitable and non-discriminatory conditions.

The Council judged that the relevant DRM markets have not yet been defined . No clear answer has been given with regards to the question of knowing if it is necessary to analyse and segment the markets by taking into account types of audio, video, computer data, and/or types of customer device (walkmans, mobile phones, personal digital assistants…).

Overall, the Competition Council judged that, with regard to the current market evolution, Apple could not be considered in a dominant position. The Competition Council recalled that it could also take into account – to some extent – the interests of users or consumers, but only if the reported infringement resulted from a practice forbidden by competition Law.In this case, the principal argument of Virgin Mega's legal action was a claim founded on the notion of essential resources and a so-called jurisprudence of essential facility.

By virtue of precedents jurisprudence, an operator can issue a claim to demand a compulsory licence, under the condition that he demonstrates that the access to a protected element, like a patent, is necessary for him to operate on the market, which means that there is no real or potential substitute to this access.

A well-known decision from the European Community Court of Justice(April 19, 2004) added that a refusal of licence could be considered abusive, if the company that demanded the licence had the intention to offer on the market devices, data, or new products or services that the intellectual property right owner did not offer, and for which there was a potential demand from customers. The Competition Council implemented this jurisprudence in the present case, and considered, first, that possible substitutes to the use of Fairplay existed, and secondly, that no characterized infringement was obvious. Moreover, the Council noticed that Virgin Mega had no intention to offer a new product or service that Apple did not offer and whose commercialisation would be conditioned by an access to Apple DRM.

In summary, the Competition Council implemented the 2004 jurisprudence of the European Community Court of Justice in a case regarding the online music market. The same parameters and criteria of competition law implemented in the framework of intellectual property law could also be implemented in the framework of DRM used on mobile phones. In its decision from November 9, 2004, which we have already mentioned, the French Competition Council explained that one of Apple's arguments (to defend its refusal to grant Fairplay licences to other operators) was that(because of certain provisions of its contracts with the Majors), if Apple should grant licences, the latter would be compelled to

maintain a total control over the DRM of the third parties, which would have been granted this licence.

This indication from Apple shows the crucial importance of contractual responsibility and negotiated security provisions.

III – LIABILITIES WHEN A HANDSET IS HACKED; WHO IS RESPONSIBLE?

We will now discuss the different possible grounds of liability, on the assumption that article 6 has been enforced and the circumvention of technological protection measures has not been helped.

Who is responsible when a handset is hacked?

- The hacker?
- The user?
- The manufacturer?
- The operator?
- The content provider?
- The content owner?

We have dedicated this part to the sole purpose of compiling texts that are useful for consideration.

1 The absence of a specific regime in the 2001 directive

1.1 No specific liability regime specified in the Directive 2001/29/EC of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society

1.2 Contractual Liability

2 The application of general liability rules found in other texts

2.1 Directive 85/374/EEC of 25 July 1985 on liability for defective products

2.2 Directive 2000/31/EC of 8 June 2000 on electronic commerce implemented by the French Law of 21 June 2004

2.3 General liability: Articles 1382 and following of the French Civil Code

2.4 Specific Telecom Laws?

2.5 Unauthorised access to an automated data processing system: Articles 323-1 and following of the French Criminal Code

2.6 Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data, implemented by the French Law of 6 August 2004 that modified the French Law of 6 January 1978

2.7 “Paris Hilton’s handset hacked”

1 The absence of a specific regime in the 2001 directive

When a handset is hacked, and a copyright file is illegally downloaded, what the grounds for liability?

Does the EC Directive on the harmonization of copyright provide a specific regime? (1.1)

If not, can an answer be found in the clauses of the contracts signed between the different parties? (1.2)

1.1 Directive 2001/29/EC of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society

As previously mentioned, there is no specific principle of responsibility on the grounds of copyrights.

The 2001 Directive does not stipulate a specific manufacturers' liability regime.

One must therefore apply the general liability rules.

This is even clearly specified in the whereas no. 16 of the Directive:

“Whereas (16) Liability for activities in the network environment concerns not only copyright and related rights but also other areas, such as defamation, misleading advertising, or infringement of trademarks, and is addressed horizontally in Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market ("Directive on electronic commerce")(4), which clarifies and harmonizes various legal issues relating to information society services including electronic commerce. This Directive should be implemented within a timescale similar to that for the implementation of the Directive on electronic commerce, since that Directive provides a harmonized framework of principles and provisions relevant inter alia to important parts of this Directive. This Directive is without prejudice to provisions relating to liability in that Directive.”

⇒ One must therefore apply the contractual (1.2) and the general liability rules (part II).

1.2 Contractual liability

A party, if it has breached one of its obligations stipulated in its contract, will be responsible on the grounds of its contractual liability.

⇒ *Comments on the contracts sent by CMLA.*

Analysis of the standard terms released by the Content Management License Administrator (www.cm-la.com).

Let’s emphasize that what is important for the companies that produce and exploit the security software, is to ensure that mobile phone manufacturers to which the licenses are granted for the purpose of exploiting the software and DRMs, do not exceed the number of copies which are the object of the authorization. Any restrictions to the scope of the authorizations must be provided for in the licensing agreements.

In terms of security, as regards whether the owners of the software or pieces of work, or the end-consumers, it will be advisable in the future to refer to a series of texts of law, in order to verify those which may be applicable.

2 The application of general liability rules found in other texts

The copyright EC Directive does not provide for a specific liability.

One must therefore search for answers elsewhere.

What other legal texts can bring answers to the question of liability?

Texts on very different subjects cover some aspects of liability:

- defective products (2.1)
- electronic commerce (2.2)
- general liability (2.3)
- telecom laws (2.4)
- unauthorised access to an automated data processing system (2.5)
- processing of personal data (2.6).

It is also interesting to illustrate this by mentioning a recent hacking of a celebrity's handset (2.7)

2.1 Directive 85/374/EEC of 25 July 1985 on liability for defective products

Article 1: The producer shall be liable for damage caused by a defect in his product.

"Whereas protection of the consumer requires that all producers involved in the production process should be made liable, in so far as their finished product, component part or any raw material supplied by them was defective; (cf. article 3: the manufacturer of a finished product, the producer of any raw material or the manufacturer of a component part)

whereas, for the same reason, liability should extend to importers of products into the Community and to persons who present themselves as producers by affixing their name, trade mark or other distinguishing

feature or who supply a product the producer of which cannot be identified; (cf. article 3 : any person who, by putting his name, trade mark or other distinguishing feature on the product presents himself as its producer + any person who imports into the Community a product for sale, hire, leasing or any form of distribution in the course of his business)

Whereas, in situations where several persons are liable for the same damage, the protection of the consumer requires that the injured person should be able to claim full compensation for the damage from any one of them; (cf. article 5 : liable jointly and severally)

whereas, to protect the physical well-being and property of the consumer, the defectiveness of the product should be determined by reference not to its fitness for use but to the lack of the safety which the public at large is entitled to expect; (cf. article 6)

…

Whereas a fair apportionment of risk between the injured person and the producer implies that the producer should be able to free himself from liability if he furnishes proof as to the existence of certain exonerating circumstances; (cf. article 7: he did not put the product into circulation; or the defect which caused the damage did not exist at the time when the product was put into circulation by him or that this defect came into being afterwards;….)

Whereas the protection of the consumer requires that the liability of the producer remains unaffacted by acts or omissions of other persons having contributed to cause the damage; whereas, however, the

contributory negligence of the injured person may be taken into account to reduce or disallow such liability; (cf. article 8)

…

Whereas, to achieve effective protection of consumers, no contractual derogation should be permitted as regards the liability of the producer in relation to the injured person; (cf. article 12)

Whereas under the legal systems of the Member States an injured party may have a claim for damages based on grounds of contractual liability or on grounds of non-contractual liability other than that provided for in this Directive;" (cf. article 13)

Article 4 : The injured person shall be required to prove the damage, the defect and the causal relationship between defect and damage.

⇒ The Directive 85/374/EEC of 25 July 1985 on liability for defective products, provides that:

- the manufacturer of a finished product;
- the producer of any raw material;
- the manufacturer of a component part;
- any person who, by putting his name, trade mark or other distinguishing feature on the product presents himself as its producer;

- any person who imports into the Community a product for sale, hire, leasing or any form of distribution in the course of his business;

are made liable for damage caused by a defect in the product.

If the conditions are fulfilled, this text may thus be referred to, notably against a defective handset manufacturer.

2.2 Directive 2000/31/EC of 8 June 2000 on electronic commerce implemented by the French Law of 21 June 2004

"Section 4: Liability of intermediary service providers

Article 12 -"Mere conduit"

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:
(a) does not initiate the transmission;
(b) does not select the receiver of the transmission; and
(c) does not select or modify the information contained in the transmission.

2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

…

Article 13 - "Caching"

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:

(a) the provider does not modify the information;

(b) the provider complies with conditions on access to the information;

(c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;

(d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and

(e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

Article 14 - Hosting

1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.
…

Article 15 - No general obligation to monitor

1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements."

⇒ This text provides that a service provider cannot be liable if certain conditions are fulfilled.

On the contrary, if the conditions are not fulfilled, the provider may be liable.

2.3 General liability: Articles 1382 and following of the French Civil Code

Articles 1382 and 1383 of the French Civil Code, which provide for general principles of liability, stipulate that:

"Any act whatever of man, which causes damage to another, obliges the one by whose fault it occurred, to compensate it". (Art. 1382)

"Everyone is liable for the damage he causes not only by his intentional act, but also by his negligent conduct or by his imprudence". (Art. 1383)

and results in the payment of damages.

The injured person shall be required to prove the damage, the defect and the causal relationship between defect and damage.

⇒ **This text has a very general scope. It may therefore be referred to, against any and all person, if the conditions are fulfilled.**

2.4 Specific Telecom Laws?

Telecom laws may also provide answers to specific cases.

2.5 Unauthorised access to an automated data processing system: Articles 323-1 and following of the French Criminal Code

Ordinance no. 2000-916 of 19th September 2000 & Law no. 2004-575 of 21st June 2004 added new articles to the French Criminal Code:

Article 323-1

Fraudulently accessing or remaining within all or part of an automated data processing system is punished by two year's imprisonment and a fine of € 30,000.

Where this behaviour causes the suppression or modification of data contained in that system, or any alteration of the functioning of that system, the sentence is three years' imprisonment and a fine of € 45,000.

Article 323-2

Obstruction or interference with the functioning of an automated data processing system is punished by five years' imprisonment and a fine of € 75,000.

Article 323-3

The fraudulent introduction of data into an automated data processing system or the fraudulent suppression or modification of the data that it contains is punished by five years' imprisonment and a fine of € 75,000.

Article 323-3-1

Anyone who - without any legitimate motive - imports, holds, offers, sales, or puts to someone's disposal any equipment, device, instrument, computer program or data, produced or specially adapted to commit one or more infractions mentioned in Articles 323-1 to 323-3, shall be punished by virtue of the infraction itself, or by virtue of the most severely punished infraction.

Article 323-4

The participation in a group or conspiracy established with a view to the preparation of one or more offences set out under articles 323-1 to 323-3, and demonstrated by one or more material actions, is punished by the penalties prescribed for offence in preparation or the one that carries the heaviest penalty.

Article 323-5

Persons convicted of any of the offences provided for under the present Chapter also incur the following additional penalties:

1° forfeiture of civic, civil and family rights, pursuant to the conditions set out under article 131-26 for a maximum period of five years;

2° prohibition to hold public office or to undertake the social or professional activity in the course of which or on the occasion of the performance of which the offence was committed, for a maximum period of five years;

3° confiscation of the thing which was used or intended for the commission of the offence, or of the thing which is the product of it, with the exception of articles subject to restitution;

4° mandatory closure, for a maximum period of five years of the business premises or of one or more of the premises of the undertaking used to commit the offences;

5° disqualification from public tenders for a maximum period of five years;

6° prohibition to draw cheques, except those allowing the withdrawal of funds by the drawer from the drawee or certified cheques, for a maximum period of five years;

7° public display or dissemination of the decision, in accordance with the conditions set out under article 131-35.

Article 323-6

Companies (legal entities) may incur criminal liability for the offences referred to under the present Chapter pursuant to the conditions set out under article 121-2.

The penalties incurred by legal persons are:

1° a fine, pursuant to the conditions set out under article 131-38;
2° the penalties referred to under article 131-39.

The prohibition referred to under 2° of article 131-39 applies to the activity in the course of which or on the occasion of the performance of which the offence was committed.

Article 323-7

Attempt to commit the misdemeanours referred to under articles 323-1 to 323-3 is subject to the same penalties.

⇒ **Articles 323-1, 323-2, and 323-3,** introduced in the French Criminal Code by the “Godfrain Law” stipulate that:

- Fraudulently accessing or remaining within all or part of an automated data processing system;

- Obstruction or interference with the functioning of an automated data processing system;

- The fraudulent introduction of data into an automated data processing system or the fraudulent suppression or modification of the data that it contains;

are punished by two to five year's imprisonment and a fine of € 30,000 to 75,000.

The hacker, but also anyone who imports, holds, offers, sales, or puts to someone's disposal any equipment, device, instrument, computer program or data, produced or specially adapted to commit one or more infractions, may have his/her criminal responsibility sought after.

2.6 Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data, implemented by the French Law of 6 August 2004 that modified the French Law of 6 January 1978

(14) *Whereas*, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and

image data relating to natural persons, this Directive should be applicable to processing involving such data;

Article 2 Definitions **(d)** *'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;*

…

(46) Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected;

(47) Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be

considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service;

…

(55) Whereas, if the controller fails to respect the rights of data subjects, national legislation must provide for a judicial remedy; whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability if he proves that he is not responsible for the damage, in particular in cases where he establishes fault on the part of the data subject or in case of force majeure; whereas sanctions must be imposed on any person, whether governed by private of public law, who fails to comply with the national measures taken under this Directive;

Article 17 Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

- the processor shall act only on instructions from the controller,
- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

Article 23 - Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

⇒ The controller, i.e. the one who determines the purposes and means of the processing of personal data, may have its responsibility incurred, notably if he/she did not take the appropriate technical and organizational measures in order to maintain security and thereby to prevent any unauthorized processing.

The recent hacking of a celebrity's handset is an illustration of the violation of security measures.

2.7 "Paris Hilton's handset hacked"

The celebrity's all in one cell-phone (camera, digital organizer and email terminal) was hacked.

The cell-phone uses the wireless phone giant's servers for email and file storage.

The hacker used an access to a database:

- to monitor a US Secret Service Cyber Crime Agent's email;
- to obtain customer password, voicemail pins, social security numbers and dates of birth; and

- to download texts, data files (pictures, private notes, contact listings,…) photos and videos, taken by users.

He was charged with computer intrusion and unauthorized impairment of a protected computer and pleaded guilty to felony charge of intentionally accessing a protected computer and recklessly causing damage.

Corporations must put two types of security into place:

- Network/technical security: it has been said that there was a security glitch in the website of the wireless phone giant, a programming flaw, a computer security flaw in the way the cell-phone servers were set up.

  → Corporations must audit their sites for security flaws, viruses, hackers,…

- Physical security: it has been said that an employee of the company was tricked into divulging confidential information.

  → Corporations face a serious security challenge: they must train employees to be watchful for social engineering (i.e. the use of deception to trick people into giving away sensitive data, usually over the phone).

Apparently, in this case, wireless phone giant suffered a breach of security and failed to notify affected customers of the breach – an action required by California's anti identity theft Law.

This story, whose value may be more of interest as a news item rather than as an example of legal doctrine, nevertheless serves as a reminder to us all that a company’s liability can be sought after on many grounds.