Chapter 24

INTELLECTUAL PROPERTY RIGHTS: THE SECURITY PERSPECTIVE

VAGELIS PAPAKONSTANTINOU
Attorney At Law, PK Partner, Athens

24.1. Introduction

Although Information and Communication Technology (ICT) practically left no field of law unaffected, very few cases have been recorded where they actually threatened the very fundamentals upon which such a particular field was constructed; Intellectual Property (IP) Law is however one of those fields that holds such an enviable distinction — once ICT fully released its potential, no principle of theoretical construction was left unharmed.

This chapter attempts to highlight only some of the numerous ways in which ICT affected, and continues to affect, IP Law: the emphasis this time is on cybercrime and security issues. In this context, a brief elaboration upon the reasons of change shall be undertaken before embarking upon the presentation of selected fields, where the most noteworthy issues have been raised (content, software, databases). The case of peer-to-peer (P2P) networks shall attract particular attention, not so much on account of their legal treatment, an issue more or less resolved by now, but because new technologies (for instance, IPTV or even VOIP) have brought them onto the surface in totally new contexts. Finally, the EU Database Right shall be briefly presented, again from a cybercrime and security enhancement point of view.

HANDBOOK OF ELECTRONIC SECURITY AND DIGITAL FORENSICS

http://www.worldscibooks.com/compsci/7110.html

In short, the relationship between ICT and IP rights is, to say the least, challenging. First, there are several occasions for conflict: holders of traditional IP rights (namely, the content industry[a]) have emerged as self-appointed keepers of the, traditional, IP scheme and are thus opposed to any ICT that challenges traditional IP norms (as controlled by them): for instance, P2P networks are to be judged illegal, unless they are equipped with Digital Rights Management (DRM) systems. Then, there are several occasions for profit while exploiting previously unchartered areas: ICT opens new sources of income for the Content Industry and others. New e-commerce methods add up to existing distribution channels for the benefit of those players in the market who can identify them; however, such "unchartered areas" usually come with a price on security. Finally, ICT constitutes in itself a difficulty with regard to its own legal treatment: software is still after several decades in the middle between copyrights and patents, while in some (European) jurisdictions databases profit from then own customised legal protection. In this contradictory and evolving environment, stakeholders change sides frequently and try to bend the rules to their own favour.

For the purposes of this analysis, however, IP Law should be perceived as inseparably connected by now with ICT and e-commerce models. This is an inherently risk-taking process — and risk gives birth to security issues. These issues are invariably technology-related and may be tackled with either in traditional legalistic ways or through technology itself. For those cases that have enough history of implementation to form "cybercrimes", the answer lies in formal legal methodologies. On the other hand, for those technologies and individuals that are involved with state-of-the-art developments, an increased security risk is to be expected, to which traditional legal action may not (or even, could not) always be of much use.

A single clarification to be made in advance relates to the, essentially, EU focus of the analysis that follows. Intellectual Property Law does fall within the First Pillar and is indeed more or less harmonised among all EU Member States. In the same context, the EU approach may not always be compatible with third-country approaches (for instance, in the case of copyright). Despite the substantial unifying efforts of international organisations (mostly, the WIPO) not every country uses the same rules when it comes to the protection of IP. The analysis that follows shall be primarily EU-focused, paying particular attention to EU regulation and case law (and legislative particularities as is the Database Right itself) while approaching the security and cybercrime issues brought by ICT on IP Law.

[a]The term "content industry" shall denote in this chapter "an umbrella term that encompasses companies owning and providing mass media, and media metadata. This can include music and movies, text publications of any kind, ownership of standards, geographic data and metadata about all and any of the above" (see Wikipedia at http://en.wikipedia.org/wiki/Content_industry).

24.2. ICT and Intellectual Property (IP) Rights

The legal scheme for the protection of IP is one of the few whose very premises have been challenged by the emergence of ICT. Because, as it will be immediately demonstrated, ICT changed the physical mechanisms used by legal theory ("works" and distribution channels), the protection of works of the intellect will never be the same. The attack on IP by ICT has been two-fold: not only have the exploitation methods of traditional assets ("works") been challenged, but also newcomers in the field (most notably, software but also databases, multimedia etc.) have demonstrated the limits of the IP rights system.

The legal response so far to these challenges has taken shape in a struggle, first, as regards already known "works" (music, text, image) to maintain well-known notions and mechanisms, by "cybercriminalising" new methods afforded by technology, and, second, as regards newcomers such as software or databases to avoid creating new fields of law but rather to incorporate, admittedly with little success so far, them into already existing categories of "works" in traditional IP law sense.

24.2.1. *The Basics of Change*

The conflict between the legal system for the protection of IP and ICT became unavoidable once the latter effectively altered the nature of the former's protected subject-matter (by digitising information) and reversed century-long practices (by adding telecommunications networks to traditional distribution channels).

24.2.1.1. *The digitisation of information*

The digitisation of information achieved by the, then, emerging Information Technology (IT) signaled the first difficulties for the copyright scheme [16]. Until that time, the copyright system for protecting IP had worked relatively successfully for over two centuries. It was first developed in the United Kingdom back in 1710; only at that time did mankind realise that works of the intellect could be of an economic value, based on their "use" by others, and therefore constituted "property" of their author (or right-holder). In this sense, the system that was then developed, and is still largely in use today, focused upon protection of the "work" of the intellect against unauthorised reproductions (copyright being essentially the right to copy). The author of a protected work under this legal scheme was entitled to compensation for each and every use (reproduction, copying) of his/her work by others.

The digitisation of information challenged the practical (not theoretical) parts of this scheme, by altering the nature of its subject-matter. Until then "works" came out essentially in the form of texts or music or drawings (or even movies). In these forms, however, reproductions (copies) of any "work" were relatively easy to control (and thus, ask for compensation): books had to be printed and sold on bookshelves, music had to be copied into vinyl and sold on record stores. All these actions of

reproduction involved cost (and thus could not be undertaken by anyone), and were controllable because of the relatively restricted distribution channels (shops) and the fragmented market (international commerce meant totally different things at the time). The digitisation of information managed the first blow to this scheme: once texts and music and pictures became digital, anyone could reproduce them at minimum cost. Evidently, the 17th century scheme, whereby any act of copying would confer money to the author of the work, automatically became obsolete: copying became so vast that the content industry could no longer control it as effectively as it did in the past. Even new (and technically challenging) "works" (for instance, movies) did not escape this global trend; once it was established that there was a market in copying and storing them in users' computers, it was only a matter of time before the appropriate (copying) technologies were unleashed to the public.

24.2.1.2. *Distribution over networks*

The emergence of networks, and in particular the Internet, managed the second, and crucial, blow to the legal scheme for the protection of IP, essentially by increasing exponentially the number of distribution channels. Until the interconnection of (home) computers was made possible, the digitisation of information alone, regardless whether annoying in itself for the Content Industry, remained inevitably "computer-isolated": any user could store tons of protected material in his/her computer, but use essentially was confined to his/her computer alone. Because networks did not exist (at least outside the academic or employment environment), any exchange of protected works with other users had to be performed physically, by means of copying onto a disc and carrying the disc to another computer in person. Consequently, even at that time the Content Industry was not particularly discomforted: although its property was digitised and copied massively, user-isolation meant that purchases of originals were not substantially affected.

Once user networks and, ultimately, the Internet emerged this was no longer the case: connected users were suddenly able to exchange "files" (incorporating unauthorised copies of protected material) without moving from their homes, at a single press of a button and at a marginal cost. Traditional distribution channels (i.e. shops) were shattered. No longer was it necessary at least for some users to purchase the original in order to digitise the work in it — the, vast, Internet community made sure that once a single user in the whole wide world purchased the original and digitised it everybody could then have it for free through a simple download [16].

To make things worse, e-commerce systems emerged that enthusiastically facilitated the exchange of files among users, namely peer-to-peer (P2P) networks; the analysis of the demise of the first attempts and their subsequent forms shall follow (see under Section 24.3). At any event, the Content Industry now had to face new e-commerce systems that demonstrated new ways of exploitation of its works.

The traditional IP system, based upon control of the "uses" of a work through control of its distribution channels, quickly became obsolete.

Nevertheless, at that point an interesting approach was adopted from a law-making point of view: rather than devising new theoretical and practical schemes to adopt to the new, irreversible, conditions, law-makers (supported by the Content Industry) stuck to the traditional IP scheme: in effect, control over distribution channels was attempted to be regained through Digital Rights Management (DRM) security-enabling technologies and the "cybercriminalisation" of new distribution channels such as P2P networks. At the same time, new ICT by-products (for instance, software or databases) were struggled into existing legal schemes (through an appropriate patching-up whenever needed) rather than introducing new legal tools: the limitations of this approach are making themselves obvious practically on a daily basis.

24.2.2. *The Case of "Content" (or "Works")*

Evidently, the changes presented above affected the traditional assets ("works") of the IP scheme, in other words, content (texts, music, audio, images etc.). New-type IP assets, such as software (see under Section 24.2.3) or databases (see under Section 24.4), presented other challenges to the traditional system for the protection of IP.

It is hard to overestimate the importance of content in contemporary markets. Content is an extremely valuable asset in itself (just imagine how much a pop hit or a bestseller is worth) and the reason of existence of all networks (the Internet included). Once we have found ways to communicate, we evidently need information to exchange: digitised content is practically the blood that runs in the telecommunications veins. Without, it, the Internet and much of contemporary television, to name only a few, would be void and irrelevant.

From this point of view, the conflict between ICT and traditional IP forces, as represented by the Content Industry, was inevitable. IT enabled the digitisation of content and telecommunications made the distribution of such digitised content easy to anyone. Unauthorised reproductions (copies) and distribution of protected material were bound to become extremely popular among Internet users (as it will be seen under Section 24.3, peer-to-peer networks). The Content Industry, whose income was severely affected by these developments, launched a counterattack to the technologies that threatened its interests (P2P Networks) and introduced technologies that would warrant application of the law (DRM systems).

Evidently, the field of law under discussion when it comes to the legal treatment of content is copyright (or, for some Continental European countries IP Law, as opposed to Industrial Property Law, essentially patents). It was therefore basic copyright legislation that ICT threatened, and it was copyright legislation that the Content Industry wishes to secure through its own ICT implementations (DRM systems).

When the first ICT technologies emerged and were put to public use the copyright system's reason of continued existence was loudly questioned by several proponents of "information is free". Under the new circumstances of an interconnected world, evidently a 17th century system whereby each copy of a work brought income to its author was no longer relevant [13]. Evidently, at the other end stood the Content Industry, a multi-billion infrastructure that came to secure a legal system absolutely necessary for its own survival. To keep the analysis short, it seems that the traditional IP system will not be abandoned, or changed, after all: the very same ICT technology that threatened its existence shall be put to its rescue.[b] While the Content Industry shall continue to sell its products and charge per "use" assisted by DRM systems (see under Section 24.2.2.1), the once proponents of "free information" are allowed to implement their ideals through the use of "open" licenses (see under Section 24.2.2.2) — the latter, however, being yet untested do present a series of security concerns.

24.2.2.1. *DRM systems as IP rights enforcement supplements*

Digital Rights Management (DRM) systems is the copyright response to challenges that are from time to time presented to it by IT. In short, DRM systems purport to ensure that reproductions of a "work" by a user conform to the respective lawfully acquired (and paid for) license. The equivalent in other industries would be for instance, a speedometer in cars pre-programmed not to go over the national speeding limit at any circumstances. The DRM systems ensure that users enjoy the copies of works they purchased to the exact extent they purchased them, by pro-actively prohibiting any circumvention of these rules. In practice, this is achieved through a two-step process: first, each individual piece of content is "tagged" with appropriate additional bits of information invisible to the user. Second, a system is implemented in the copying process that controls the reproductions of such, tagged, content (either by "locking" the copying machines or by reducing the quality of the content once it is copied in an unauthorised way). The DRM systems ought to be considered outside of the on-line environment: their predecessors first made their appearance in VCRs during the 80s and are still present in the off-line world, for instance, having divided the world into "zones" for DVD-related purposes.

The DRM systems are, therefore, the Content Industry's IT solution to the problems caused to it by that same IT.

Intellectual Property Law embraced DRM technologies. Ever since the digitisation of information made copying easy, even before networks aggravated the situation, appropriate amendments were made to the law in order to secure the Content Industry's interests. However, this is done in an indirect way. As far as IP Law is concerned, only "*technological measures that restrict acts unauthorised*

[b]In one yet confirmation of Lessig's "code is law" (in Code v2, available at http://codev2.cc/).

by authors", the so-called Technical Protection Measures (TPMs), are explicitly acknowledged and protected. In this context, according to the WIPO Copyright Treaty,[c] "*contracting parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorised by the authors concerned or permitted by law*".[d] The TPMs are thus passively protected in the wording above, by means of an explicit recognition of their existence in the Treaty. This is, nevertheless, not the only layer of protection afforded to TPMs: in addition to their passive protection, they are also actively protected against (in the case of e-commerce, at least) "hackers": "*contracting parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts knowing [. . .] that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty or the Berne Convention: (i) to remove or alter any electronic rights management information without authority; (ii) to distribute, import for distribution, broadcast or communicate to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority*". The TPMs (regardless whether in the e-commerce context or other) are thus protected two-fold: first, their existence is explicitly acknowledged in the text of law; second, anybody who tempers with them or anybody who passes along content whose TPM have been tempered with, shall be persecuted.

The obvious question now relates to the relationship between TPM and DRM. Despite the fact that certain views have highlighted their differences (in most of cases with an ultimate aim of justifying attempted circumventions of DRM systems[e]), judging even from their wording their actual relationship becomes clear: TPMs are the technical measures upon which DRM is based. In other words, TPM corresponds to the first of the two-step process described above: the "tagging" of individual works with additional bits of information in view of their later use in DRM systems. And, by the same token, if the act of attaching TPM onto content is recognised and protected by law, most certainly the introduction of DRM rules for the use of such (TPM-enriched) content is also, indirectly, equally recognised and protected. The use of DRM systems, regardless whether off- or on-line, is therefore, technically, lawful under IP Law.

[c]Its provisions, with regard to DRM at least, have been implemented in the United States through the Digital Millennium Copyright Act (DMCA), and in Europe through Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, commonly known as the EU Copyright Directive (EUCD) or the Information Society Directive (Infosoc).

[d]Art. 11 WCT.

[e]See, for instance, the, largely legalistic, argumentation whether TPM that can be circumvented can be "effective" or not, in order to infer whether they are protected by the WCT (see, however, Art. 6 par. 3 of the EU Copyright Directive).

This is more or less the situation by now both in Europe and in the United States. In Europe, the Copyright Directive[f] devotes a whole Chapter (Chapter III) to the "*Protection of Technological Information and Rights-Management Information*". In this context, the Directive's Articles 6 and 7 repeat, in effect, the WIPO Treaty's provisions seen above. In the United States, Section 103 of the Digital Millennium Copyright Act (the so-called "*anti-circumvention provisions*") effectively implemented the same WIPO Treaty provisions. It is therefore safe to say that by now the lawfulness of DRM systems according to IP Law and as far as its scope is concerned should be taken for granted, both in the off-line and in the online environment.

The above by no means evidence the lawfulness of contemporary or future DRM implementations. The DRM systems constitute systems that essentially reflect the business practices of their owners. The IP Law is only allowed to go as far as to validate the lawfulness of the existence of DRM technologies per se. The law cannot say whether a particular, essentially e-commerce model, implemented by a corporation is lawful, in other words, whether the rules for the use of content implemented by DRM technologies conform to IP Law provisions. This is something that should be assessed each time on an ad hoc basis, while taking into consideration not only IP Law but other fields of law that might be potentially relevant (for instance, Data Protection Law, Competition Law etc.).[g]

24.2.2.2. *"Open source" initiatives: the case of the creative commons license*

At the other end of strict DRM rules and heavily regulated content provision stands the, relatively recent, "open source" movement. Proponents of the notion of "freedom" inherent in the new medium (the Internet, but all ICT as well) have undertaken formal initiatives to assist their ideas once it became evident that the copyright scheme is here to stay, despite the assault unleashed upon it. Naturally, the most popular initiative in this context relates to the open source software, that will be discussed later in this chapter (see under Section 24.2.3.2); here, its equivalent in relation to content shall be briefly elaborated.

As far as content is concerned, the path to its free delivery to users is paved these days mostly by the Creative Commons initiative. A number of parallels may be drawn between it and the software open source movement: in the case of software

[f]Directive 2001/29/EC (the EU Copyright Directive).

[g]See, for instance, the numerous legal adventures of the, dominant in the market for the time being, Apple's iTunes. Having started out with a business model of "closed" DRM technologies that only allowed reproduction on iPods and prices that vary in different countries (not allowing inhabitants of one country purchases from its on-line store in another), after successful attacks by European organisations they have, at the time these lines are written, changed into a more open DRM system, allowing reproduction on other mp3 players and even selling (for a higher price) non-DRM content, while their pricing differentiations at least within the EU shall most probably need to be abandoned soon, after scrutiny by the competent EU authorities has begun.

the General Public License (GPL, currently in its version 3) is released by the Free Software Foundation for use by all software developers who wish their programs to be made available free (or, at least, outside a number of copyright restrictions) to the public. In the case of content, a set of (altogether six) Creative Commons Licenses are released by the Creative Commons Organisation for use by all content rightholders who wish that it is made available outside a number of copyright restrictions (depending on the type of license) to the public.

Seen under this light, the Creative Commons Licenses came to fill a gap in the (on-line) market. New artists or even established ones that do not care much about the Content Industry are given the chance to make their works available to the public under fewer copyright restrictions, exactly in the same way as software developers have been able to do for years. Nevertheless, the Creative Commons system suffers from an inherent difficulty that may ultimately threaten its existence altogether: content is far more complex than software. Content may include anything from text to images or music; it can be a single work but the norm is that it will be a composite work incorporating more than one work in it (and respective sets of rights). For instance, a picture of friends uploaded on a social networking website includes the rights of the photographer but also the rights of the persons appearing in it. Accordingly, a typical video uploaded on-line shall include images as well as music, all bearing different sets of right. In all these cases, the rightholder who makes available a work under the Creative Commons License must warrant to all those who are prompted to use it that all rights in the work are secured — a far from straightforward task, given the complexity of a typical work.[h]

At any event, the Creative Commons organisation is set, in its own words, to define "*the spectrum of possibilities between full copyright — all rights reserved — and the public domain — no rights reserved. Our licenses help you keep your copyright while inviting certain uses of your work — a "some rights reserved" copyright*" [5]. In this context, it has released a set of six different licenses to be used by authors depending on the uses they would like their works to be put to; technical guidelines are intended to assist them while incorporating these licenses (naturally, on an "as is" basis) onto their works. The first Creative Commons license is named "Attribution" and only retains the author's moral rights upon his work, while users are free to do whatever they want with it. The second Creative Commons license is named "Attribution Share Alike" and, on top of "Attribution", asks that all new creations are licensed under identical terms (in effect this type of license is paralleled to the GPL software license). The third Creative Commons license is

[h]This is after all one of the first conflicts caused by a work used under a Creative Commons License: a photographer made a picture of a girl available under a CC license and the photograph was used in an advertising campaign by a big company, only to find out that the girl's parents objected to their daughter's picture being used in this way. The case was eventually settled, but is typical of difficulties inherent in content uses that may come in the future (see http://lessig.org/blog/2007/09/on_the_texas_suit_against_virg.html).

named "Attribution No Derivatives" and, evidently, allows only for the distribution of a work on an "as is" basis. The fourth Creative Commons license is named "Attribution Non-commercial" and, equally evidently, prohibits any commercial use of a work. The fifth Creative Commons license is named "Attribution Non-commercial Share Alike" and it combines the obligation to distribute only for non-commercial purposes with the obligation to distribute under exactly the same terms (in effect abolishing any commercial uses even in licensed derivative works, an option available under the "Attribution non-commercial" License). Finally, the sixth Creative Commons license is named "Attribution Non-commercial No Derivatives" and is expressly the most strict of them all, effectively allowing mere re-distribution of a work (serving thus mostly advertising purposes) [6].

Unlike the Free Software Foundation, Creative Commons has developed a strong international orientation, with "porting" processes for its licenses (practically, however, only one of them) developing in parallel in several countries of the world. Nevertheless, given the complexity of content per se and, perhaps, the complexity of the 6-license system (that a non-legal person shall probably struggle to come in terms with), it remains to be seen whether they shall eventually become as successful and established as their GPL equivalent.

24.2.3. *The Case of Software*

Software per se is probably the most important addition to the copyright scheme during the last century (and, allegedly, the most controversial one too). Notwithstanding whether a "work" or "product", software emerged during the second half of the 20th century and came to constitute an invaluable asset within a very short period of time. Its legal treatment became thus imperative: two were the obvious options, one referring to its inclusion within already existing legal schemes and the second pertaining to creating a new legal tool. Without over-expanding on the subject, the first option was finally chosen: software was to be protected as "literary work" within the context of copyright; the limitations of this approach are making themselves obvious every day [19].

Software has always been an uncomfortable guest in the copyright legal system. First of all, rather than fitting-in, a series of specialised adjustments had to be made in order to accommodate some of its "functional" characteristics [19]. Then, the level of protection afforded by the copyright scheme to software was always considered inadequate by the software industry: in fact, only the interface (the "expression") of a computer program may be copyrighted — the source code is largely not protected and the algorithms underneath are most certainly left out of the copyright scope. These limitations, coupled with its market value, have turned the major players in the software industry towards patents, an approach that created even more problems (as will be shown under Section 24.2.3.1).

On top of said difficulties when it comes to protecting software under the copyright regime comes the multitude of its forms. Software has since its first

appearance exited the computer environment, to become present all around us. Today, apart from the inside of computers, software may be found in mobile phones, DVDs, cars, homes etc. The notion of "ubiquitous computing", when computing shall happen constantly around us without us taking notice any more, is steadily leaving research environments to enter mainstream vocabulary. And, evidently the building component of such ubiquitous computing will be software.

In this context, it appears had to perceive software still as "*literary work*", according to its legislative treatment under the copyright scheme. Rather than a "*work of the human intellect*" software has become an everyday tool divided in components and sold as a whole or as subsets performing a single function, sold off-the-shelf or bespoke, incorporated in machines or intended to be traditionally "run" on computers, residing locally or in the cyberspace. Accordingly, its functions practically encompass by now the whole of human activities, including work, home and entertainment environments. The common factor of all the above is, evidently, more a "product" than a "work", more an industry than art.

Within this environment the security connection is inevitable. Even if one is not ready to acknowledge that "code is law" [12], the more software is used in domains of human life the more security add-ons shall be enabled in it in order to make this, socially, possible. E-commerce systems, for instance, would have been void of any (consumer) interest if appropriate security mechanisms for tracing fraud and executing a lawful transaction were not in place. Such systems evidently include mechanisms both for prevention of mishappenings and for detection of the culprit if, despite all measures to the contrary, a breach is identified. Adequate security systems, that will not only be robust but also look that way to the public, are of central importance to any software implementation regardless whether used for profit (e-commerce systems, web banking systems etc.) or other purposes (privacy protection, state security etc.). Public trust in new technology implementations is only gained through adequate security measures installed therein.

Apart from add-ons on software applications intended to increase or create security and public trust, one must not forget that software per se is an asset of great value that is, unfortunately, easily copied. Security measures are thus attached in it too in order to discourage this possibility (in the same way that DRM systems operate for content). Again such mechanisms should aim both at prevention and at detection against what essentially constitutes "*software piracy*".[i] Software piracy, despite appearances, has not always been at the top of the industry's agenda,[j] because, especially back in the 80s, distributing inadequately protected software was a shortcut for securing a wide customer basis. This largely explains the mediocre level of security with which the software industry even today protects

[i]For a definition of "software piracy", see http://www.bsa.org.

[j]The Business Software Alliance organization ("*the foremost organization dedicated to promoting a safe and legal digital world*") was only established in 1988 (see http://en.wikipedia.org/wiki/Business_Software_Alliance).

its products from unauthorised copying (if, for instance, compared with aggressive DRM technologies used by the Content Industry). Security concerns thus, when it comes to software per se, are mostly addressed by legal means, when a breach of the respective End-User License Agreement (EULA) is indeed identified and the offender is called to indemnify the infringed party.

Finally, the making of unauthorised copies is not the only way software may be involved with crime. Software is frequently used as a tool to commit crime, in or out of the computer environment. Two distinctions may be drawn in this case: crimes that are committed with the assistance of software developed especially for this purpose, or crimes that are committed on software. The first category will generally refer to any technologies designed to, for instance, steal credit card numbers, make unwanted calls, open holes on security systems etc. The second category involves unauthorised access to computers and tampering with their software (for instance, computer hacking) regardless whether for profit or not. Here again, security measures are expected to be aimed both at preventing such actions and, if committed, in assisting detection of the culprits.

It, therefore, becomes clear that software is called to assume a multitude of roles. First, it has to adequately protect itself and its economic value. Second, it has to adopt in various social and technical environments, securing public trust through adequate prevention and detection mechanisms. Third, software often becomes the crime itself, when either put to this cause or "suffering" from the crime. The complexity of this situation is only marginally assisted by software's current legal treatment under the copyright scheme, as a "literary work", a legal solution nevertheless that seems to have missed the need for change.

24.2.3.1. *Patents*

Patents, when related to copyright, stand at the opposite side of the IP spectrum. In principle, the two systems were never meant to intersect (and, indeed, in Continental Europe, at least copyright falls within IP Law and patents fall within Industrial Property Law, two entirely different fields): copyright was the devised mechanism to award creativeness when it comes to "works of the intellect" (books, pictures, music etc.), whereas patents were themselves invented in order to protect machines indented for industrial use. Software blurred the distinction, because, despite of the fact that it is placed under the copyright scheme as "literary work", it presents elements that not only constitute a "work of the intellect" but are also used as "tools" in everyday life. Additionally, copyright notoriously protects very little out of a typical computer program (in effect, only its interface), whereas patents, if awarded, go as far as protecting the algorithm (evidently, for that particular use). It is in view of the above that, first, a number of software or software-like inventions have been awarded patents despite the rules to the contrary, and, second, many regulatory initiatives have been undertaken towards patentability of software, that have been, nevertheless, all unlucky so far.

From this point of view, any security issues concerning software per se when it comes to the dispute between copyright and patents will inevitably follow the above, or any future, developments. As long as software continues to be protected by copyright, as is currently the situation, great use for digital (computer) forensics tools shall lie with regard to copyright infringements: because copyright does not protect the algorithm and only a substantial portion of the source code, minor modifications among competitors that essentially launch the same product are to be expected. All these cases present an evident security interest while, for instance, evidenced in court. The same applies to patent-protected software: any unauthorised use will have to be supported by sufficient digital (computer) forensics-provided data. On the other hand, the software industry shall continue its efforts to equip their software tools (for the purposes of this analysis, DRM technologies etc.) with patents in order to better protect them against competition [15].

24.2.3.2. *Open source software*

The notion of open source software, being by now in its version 3 of its most popular EULA (the GPL) need not be presented here; here it is enough to be noted that open source software is the response (of, mostly, the developers' community) to proprietary software — rather than locking the code of a computer program, a typical open source alternative provides access to its source code and the freedom, under certain conditions, to edit it. Open source software affects the electronic security field in more than one way: first, it is a potential field of digital forensics implementations in itself, while, for instance, establishing adherence to the EULA (GPL) terms and conditions. Second, open source tools have been made available for the digital forensics field, whose effectiveness, however, needs to be evidenced. Finally, the notion of the open- or open-source domain and advanced search options have already posed previously unknown security/intelligence issues.

As far as open source software per se is concerned, the freedom-to-use principle has already given birth to a number of disputes, particularly with regard to adherence to the inevitable respective conditions. The fact that a computer program is made available on an open source basis does not necessarily mean that conditions for its use do not apply as well. For instance, the GPL license asks that any software using software provided under its terms and conditions is, in turn, made available to the public under the same, GPL, license (Section 2). This principle, the so-called inheritance principle, constitutes one of the most widely disputed issues relating to the open source scene. While the software market and the software industry challenge its validity, because of the obvious restraints it creates for their business development, the open source proponents (mostly, the Free Software Foundation) are ardent supporters of its fair character and justified use in practice. It is in this context that software made available to the public under any version of the GPL license carries this burden. Nevertheless, once in a while proprietary software emerges that allegedly uses GPL-licensed software without observing the inheritance

principle (that would, in effect, make it as a whole or part of it open source as well). It is in these cases, where the actual use and the extent of incorporation, if any, of GPL-licensed software in proprietary software is to be established, that digital (computer) forensics tools inevitably hold a central role.

The digital forensics field is in turn affected by open source tools. Open source tools are claimed to have a legal benefit over closed source tools because they have a documented procedure and allow the investigator to verify that a tool does what it claims [8]. In these cases, however, the effectiveness of such tools, when used in certain conditions, needs to be validated [3].

Finally, the notion of the "open source" domain, where information is posted on-line in a simple way for everyone to use, when combined with powerful search tools that are also freely distributed over the Internet create a powerful outcome with serious security implications from an intelligence gathering and processing point of view [18]. Again, in this case, procedural and substantial measures need to be undertaken in order to monitor the flow of information from security-sensitive fields in the free, on-line environment.

24.3. P2P Networks and Their Effect on the Law

As already seen, the distribution of content over networks gravely affected, if not threatened, the premises of IP Law: once digitised content was exchanged by users over networks (the Internet), the traditional scheme for the protection of IP and the Content Industry itself were never going to be the same. The story of the first P2P networks, and their ultimate judicial demise, is by now known to everybody, therefore here it shall be briefly elaborated: P2P networks emerged once the Internet found its way into the homes of users and constituted a, then novel, e-commerce method: the network facilitator only made its infrastructure available to individual users who exchanged (mostly copyright protected) content and profit was made through advertisement. This e-commerce business method in effect created a mass copyright infringement, whereby millions of users exchanged millions of, then, songs around the world. The battle between the Content Industry (as represented by its music branch) and new e-commerce players (P2P networks) was fierce and lasted a decade. Although a number of cases were initiated by music labels against P2P networks, the one that finally did make it to the US Supreme Court was the one by Metro-Goldwyn-Mayer against Grokster. The question at hand was whether a P2P networks facilitator could be held indirectly ("secondary") liable for the uses of its software by its users (that is, for the unauthorised exchange of copyrighted material among its users). At first[k] the P2P operators seemed like they could get away with it: courts were confused with the, then relatively recent VCR cases, where VCR manufacturer Sony was not held responsible for copying of TV shows

[k]Court of Appeals (Ninth Circuit) 380 F 3d 1154.

performed by users using its sets,[l] and drew the analogy between this case and P2P networks facilitators. Nevertheless, the US Supreme Court held otherwise[m]: based on quantitative and qualitative criteria (for instance, 90% of content stored on P2P networks is copyrighted material, 100 million users exchanged more than 1 billion files on a monthly basis, plus the fact that P2P operators actually advertised this aspect of their systems) it decided, in short, that P2P networks operators are ultimately liable for the actions of their users, and thus made the continuation of their operation in their then form no more viable.

The, American, verdict on Grokster unavoidably affected the way all countries around the world viewed P2P networks, "cybercriminalising" in effect all their known at the time forms. By the time this analysis was written, P2P facilitators, at least in their previous form, were more or less abolished from the Internet. In the meantime, legal implementations, for instance Apple's iTunes, dominated the Internet, providing users with the opportunity to download and use content in a legitimate way.

P2P technology, however, was not abolished as well. Quite on the contrary, it constituted and continues to constitute a widespread technology used for a multitude of purposes. The only part of it that was judged unlawful in the Grokster case was the encouragement of users to trade unlawfully copied content; if, however, ways were devised that such downloads be made legal, then the technology would be perfectly lawful. Additionally, other fields, such as Internet telephony (for instance, Skype) may use the same technology at its basis.

Nevertheless, the very nature of P2P networks makes them a security nightmare. Their "shared" character, whereby each user uses them in any way he/she pleases and the facilitator has practically no way of centrally controlling or even monitoring such uses, inevitably leads to serious security implications. P2P networks, under their contemporary legal treatment and using contemporary legal schemes, are bound to present a series of security threats, at least when seen from, for instance, the Content Industry (when it comes to music or video sharing) or the state (when it comes to Internet telephony) perspective.

As far as their file exchange function is concerned, P2P networks may (or may not) have struck the correct balance between user exchange of content and copyright adherence through the implementation of DRM (e-commerce) systems. As already seen, these systems constitute the technical, but not necessarily legal or even business, reply to widespread Internet distribution of content through P2P networks. As soon as it is established that such exchanges are lawful, through the exchange of DRM-protected material, P2P networks may continue to thrive based on their technological advantages. It is in this context that, for instance, WebTV initiatives such as Joost have been released: P2P technologies equipped with DRM security for content aim at the Internet public [7].

[l] *Sony Corp. of America v. Universal City Studios Inc.* 464 US 417 (1984, BETAMAX case).
[m] *Metro-Goldwin-Mayer Studios Inc. et al. v. Grokster Ltd., et al.*, 27 June 2005.

The limitations, however, of using DRM technologies over P2P networks are already making themselves felt. DRM technologies are thought to be too much restrictive in the Internet context,[n] and the Content Industry has been accused of not understanding the new medium. Once the Grokster case has established that P2P facilitators could no longer operate in the way they used to, the Internet community pressed for continued use of P2P networks in a lawful way. The Content Industry (music, but ever increasingly video as well) is pressed to devise ways of distributing content making use of P2P networks or other on-line channels in an efficient and lawful way for users; its existence itself is said to depend on its ability to adopt into the new reality. For the time being, such voices have not been heard, and DRM-equipped P2P (or other) networks appear to be the only contemporary lawful solution for the on-line provision of content; the situation may, however, change drastically in the future.

As regards other implementations of P2P technologies, Internet telephony (VOIP) has attracted particular attention. P2P technology is the basis upon which such popular solutions such as Skype are built.[o] However, regardless whether over the Internet or not, telephony remains a telecommunications service from a state/public security perspective. In Europe, various regulatory initiatives have been adopted for the processing of telecommunications data, the most well-known of which is probably by now the Data Retention Directive.[p] Such a Directive asks that, particularly with regard to Internet telephony, a series of personal data (user ID, telephone number, IP address etc.) be kept by the service provider for periods from six months up to two years.[q] However, here again the inherent "shared" nature of P2P networks, upon which VOIP is based, present a series of security issues: in effect, governments find it increasingly hard, if not impossible, to monitor Internet phone calls, even if they have the lawful right (and have followed the lawful procedure) to do so [4].

It therefore becomes evident that P2P technology is found at a constant conflict with the law. Its "shared" nature presents inherent security difficulties that are not dealt with efficiently under contemporary legal schemes. Under the regulatory framework in effect, user sharing of content over P2P networks shall continue to be illegal, while VOIP shall continue to grant criminals with intolerable potential as to their secure communication. "Cybercriminalising" appears thus to be the legal

[n] Indeed, for instance, Apple's iTunes are already making DRM-free content available through their service for an increased fee.

[o] See http://www.skype.com/help/guides/voip and Salman A. Baset and Henning G. Schulzrinne, An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol, available at http://www.eecs.harvard.edu/~mema/courses/cs264/papers/skype-infocom2006.pdf.

[p] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105/54, 13.04.2006 (available under http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2006/l_105/l_10520060413en00540063.pdf).

[q] Art. 5 and 6 of the Data Retention Directive.

response to P2P networks so far. On the other hand, contemporary legal schemes that were devised at times when networks did not exist or were at least state-restricted and controllable (such as, for instance, the standard telephony networks) may be by now obsolete, crushed under wide Internet connections available to everyone for a marginal cost and individuals' inherent need to communicate globally. It remains thus to be seen whether in the future P2P networks shall be subdued to contemporary (IP and other) legal restrictions, or whether the need for a novel regulatory approach shall be identified and adopted, in order to better accommodate a newcomer that, for all its judicial troubles, has proven extremely resilient and adopting and is evidently here to stay.

24.4. The EU Database Right

The *sui generis* Database Right is an EU law exclusivity. Back in 1996, when it was established that the European database industry was lagging behind its American and Japanese competitors, it was felt that an adequate regulatory boost would be given by introducing a new, special (*sui generis*) right particular to the needs and particularities of databases[r]: the outcome was the Database Directive,[s] implemented by now into the national law of all EU Member States. The Database Directive essentially establishes that databases are indeed protected by copyright, under IP Law; those of them, however, that do not qualify for such a protection may profit from the new, *sui generis*, Database Right. And, quite a few of them may not profit from copyright protection: because copyright is awarded to "works of the intellect" that must present some originality and uniqueness (even at such low levels as computer programs are allowed to), most databases, whose added value lies most on the breadth of their contents and not their creation will generally fail the test. In addition, even those that do pass the test may still find it hard to abide by copyright rules, whereby fees are due for each complete reproduction of a work rather than access to part of it. At any event, the Database Directive became European law at a time, in the late 90s, when the online and, broadly speaking computer, environment[t] made a new market, that of databases, possible.

Given that the Database Directive was expressly not to be confined within the computer-automated environment,[u] the breadth of its scope was, originally at least, astonishing. Indeed, under the Database Directive such collections as dictionaries, single webpages cataloguing information or even web links, exhibition catalogues, the newspaper classifieds, or even the public tenders published in the financial press may be considered as a protected material. The only substantial limitation to widespread application of the Directive came later, through case law of the

[r]See Recitals 11 and 12 of the Database Directive.
[s]Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 077, 27/03/1996.
[t]See, for instance, Recitals 9, 10 or 13 of the Database Directive.
[u]See Recital 14 of the Database Directive.

European Court of Justice (ECJ). In a well-known case,[v] the ECJ stressed upon the importance of the distinction between "creation" of a database and "obtaining, verification and presentation" of its contents. In effect, in order for a database to qualify for the *sui generis* database right, its owner must have spent substantial resources while either obtaining or verifying or presenting its contents — merely spending money for its creation will not suffice. This ruling left out of protection such cases as phone books or, as was the disputed subject-matter, betting listings.

Regardless of the above restriction in its scope, the fact remains that the Database Directive constitutes a powerful tool in the hands of owners of compilations, both in the online and the off-line environment. Particularly over the Internet, where substantial work may have been put to compiling webpages and publishing freely (with an aim to make profit through other means), Internet site owners may find themselves at a disadvantage, being squeezed between strict copyright requirements and broad unfair competition provisions. Practices, for instance, such as framing or deep-linking may effectively be dealt with under the database, *sui generis* right, regulatory framework (see Chapter 35, . . .). On the other hand, although beneficial to the arsenal of lawyers, it remains to be seen whether the database right shall indeed at some point in the future serve its proper purpose, that is to boost the European database market,[w] or whether it shall remain a legalistic alternative to a series of more or less already known and accounted for e-commerce practices.

References

1. D. Bainbridge, *Intellectual Property*, 6th Edition (Longman, 2006).
2. L. Bently and B. Sherman, *Intellectual Property Law*, 2nd Edition (Blackstone Press, 2004).
3. B. Carrier, Open source digital forensics tools: the legal argument, available at http://www.digital-evidence.org/papers/opensrc_legal.pdf.
4. A. Gavras, Security weakness of VoIP, 2007, available at http://www.eurescom.de/message/messageMar2007/Security_weakness.of-VoIP.asp.
5. http://creativecommons.org/about/.
6. http://creativecommons.org/about/license/.
7. http://www.joost.com/forums/f/p2p-technology/.
8. http://www.opensourceforensics.org/.
9. P. Leith, *Software and Patents in Europe* (Cambridge University Press, 2007).
10. L. Lessig, *Free Culture*: *The Nature and Future of Creativity* (Penguin Books, 2005).
11. L. Lessig, *Code*: *Version 2.0* (Basic Books, 2006).
12. L. Lessig, Code is law, Code v2, available at http://codev2.cc/.
13. L. Lessig, Free culture, available at http://www.free-culture.cc/.
14. I. Lloyd, *Information Technology Law*, 4th Edition (LexisNexis UK, 2004).

[v]European Court Justice, *British Horseracing Board v William Hill*, C 203/02, [2005].
[w]See DG Internal Market and Services Working Paper, First evaluation of Directive 96/9/EC on the legal protection of databases, 12 December 2005, available at http://ec.europa.eu/internal_market/copyright/docs/databases/evaluation_report_en.pdf.

15. Microsoft patents digital audio DRM watermark, 2007, PC Advisor, 12 September 2007, available at http://www.pcadvisor.co.uk/news/index.cfm?newsid=10696.
16. P. Petrick, Why DRM should be cause for concern: an economic and legal analysis of the effect of digital technology on the music industry (November 2004), Berkman Center for Internet & Society at Harvard Law School Research Publication No. 2004-09. Available at SSRN: http://ssrn.com/abstract=618065.
17. C. Reed and J. Angel, *Computer Law*, 5th Edition (Oxford University Press, 2003).
18. D. L. Watson, Stealing corporate secrets using open source intelligence (the practitioner's view), *Int. J. Electronic Security and Digital Forensics*, **1**(1) (2007) 71.
19. R. Widdison, Software patents pending?, *The Journal of Information, Law and Technology (JILT)* 2000 (3). <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/widdison/>.