Fencing Copyrighted Content off in the Digital Age. The Case for Technological Fences ("Trusted" Computing in Particular) and the Legal Infrastructure in Support of Them: A Cautionary Note.

Ioannis G. Valmas

Athens, Greece, 2003-2009

Contents

Acknowledgements

I wish to thank everyone at the Law Department of the University of Wales, Aberystwyth for their support during the course of my studies. Special thanks to Richard Ireland, without whose support I would not have been part of this course, and Uta Kohl for her patience, immediate responses, and insightful comments during the course of my research. Many thanks to Professors: Yochai Benkler (Yale Law School), William Fisher (Harvard Law School), Lawrence Lessig (Stanford Law School), Charlie Nesson (Harvard Law School), Jonathan Zittrain (Harvard Law School), all of whom – during the course of the 2003 i-Law Program (Stanford Law School, Palo Alto, California) –, provided some excellent feedback (through their tuition and suggesting reading material) for the essay that follows. The views expressed in this essay, however, are the author's views (unless otherwise stated), and any omissions are to be debited to the latter. Last but not least, thanks to my family for their wholehearted support during the course of my studies.

Aberystwyth, UK, March 2004

Abstract

This essay examines the legal and technological infrastructure that is currently developing in order to combat piracy of intellectual property creations in digital form. Trusted Computing is a technology that, when combined with the current legal infrastructure that is developing, could help the content industry (right holders) to successfully control and condition access to intellectual creations in digital form.

There are two main camps of thought in relation to combining legal and technological solutions in order to update copyright law. On the one hand, there are those who wholeheartedly support the combination of legal and technological means of protection of intellectual property in digital form. This camp includes lawyers, the content industries, and the technology industries involved in the development of trusted computing.

On the other hand, there are those who – like with the above – understand the need for devising a copyright scheme that will guarantee protection for right holders' legitimate rights; however, this should be subject to important qualifications. If the content and technology industries are given (by the technology they advance and the law) too much power in the making of copyright policy, there is a potential for abuse of this power. Hence, most of this work will

examine the ways with which the content industries could abuse this power that laws are currently granting to technological means of intellectual property protection such as Trusted Computing.

It is therefore argued that copyright policy should not narrowly focus on the private interests of right holders. Values such as societies' progress, openness, transparency, and the respect of certain rights and freedoms (such as the right to privacy) should go hand-in-hand with copyright policy in the context of current technological and legal developments. Bad implementations of law and technology may threaten these values. We will therefore need to safeguard that we will preserve and build upon these public values in the context of making copyright policy in the digital age.

Prologue

"Out there on the electronic frontier, **code is the law**. The rules governing any computer-constructed microworld – of a videogame, your personal computer desktop, a word processor window, an automated teller machine, or a chatroom on the network – are precisely and rigorously defined in the text of the program that constructs it on your screen. Just as Aristotle, in *Politics*, contemplated alternative constitutions for city-states (those proposed by the theorists Plato, Phaleas, and Hippodamos, and the actual Lacedaemonian, Cretan, and Carthaginian ones), so denizens of the digital world should pay the closest of critical attention to programmed polity. Is it just and humane? Does it protect our privacy, our property, and our freedoms? Does it constrain us unnecessarily or does it allow us to act as we wish?" **W. J. Mitchell**[1]

William Mitchell's words have been highly influential, and thought provoking. His views, as well as Lawrence Lessig's subsequent book entitled *Code and Other Laws of Cyberspace*[2] have been the inspiration for this essay, as the contention that *code is the law* – used by both academics – provides the basis for the analysis that follows. This essay, however, will more narrowly focus on a specific architecture and its implications on the global information society: **Trusted**

[1] **See** William Mitchell, ***City of Bits – Space, Place, and the Infobahn***, The MIT Press, 1995, p. 111.

Computing. Trusted Computing is a computing platform that aims to fence copyrighted content through personal computers' software and hardware. Through the development of trusted systems, content owners could be able to define the scope of uses of copyrighted content by consumers of information. For example, once digital publishing has become widespread, content owners may be able to define whether a consumer of an information product – such as a digital book – will be able to copy the book, and how much of it, or determine how many times it may be read. Current Internet use suggests that, for example, with regards to digital music files, there is an increasing amount of pirated content circulating within the Internet. Content owners need to safeguard that their content is protected. Trusted Computing, the development of trusted systems that is, might be a significant step towards combating piracy.

On the other hand, the implementation of technologies such as Trusted Computing may lead to problems. Copyright has been a bargain between public and private interests; it is a trade-off between the two. There is a delicate balance that needs to be struck and handing the regulation of copyrights to the technology and content industries may lead to a situation that may tip the balance in favour of established interests.

The first chapter of this essay will examine how it is possible to fence copyrighted content through trusted computing technologies and how such technologies might regulate behaviour with a view to hidden regulatory objectives. As it will

[2] **See** Lawrence Lessig, ***Code, and Other Laws of Cyberspace***, Basic Books, 1999. Lawrence Lessig has worked on many of Mitchell's ideas and has provided us with a deeper understanding of the interrelation of **code** and **law**.

become apparent the possibilities and opportunities for abuse by the content industry in particular are many.

The technology might not suffice on its own in the process of fencing copyrighted content though. A legal infrastructure is currently developing that aims in aiding the above technologies in becoming widespread. The second chapter will examine how the law has, in recent years, come to the aid of the content industry. While adopting these laws[3], nations should be cautious. As it will become apparent, bad implementations of laws designed to aid trusted computing may further tip the balance in favour of established interests.

The third chapter of this essay is about several fundamental public values that must be respected and preserved during the development of both the technological fences and the legal infrastructure examined by the first two chapters. Progress, openness, transparency, and the respect of certain rights – such as the right to privacy – are values that should be quintessential in modern democracies. The European Union's draft Constitution[4] for example acknowledges the fundamental importance of the above values. Trusted Computing in turn may present a challenge to these values. We need to see how this is so; the third chapter is dedicated to this end.

---

[3] ***See***, The WIPO Copyright and Performance and Phonograms Treaties, available at: http://www.wipo.int/treaties/ip/wct/index.html. The World Intellectual Property Organisation has been the driving force behind the Digital Millennium Copyright Act in the United States of America, and the Copyright Directive (Directive 2001/29/EC) in the European Union.

[4] ***Treaty Establishing a Constitution for Europe*** (Draft),The European Convention, CONV 850/03, Brussels, 18 July 2003.

Chapter 1: The Infrastructure of "Trust"

"With the development of **trusted system technology** and **usage rights languages** with which to encode the rights associated with copyrighted material, authors can have more, not less, control over their work. **Mark Steffik**[5]

1.1. Publishing Online – Contemporary Issues

Publishers, so far, have been hesitant in distributing content online to consumers. The proliferation of file-sharing servers, such as Napster™, in the late 1990's, or their more sophisticated "clones" (peer-to-peer[6] networks) that, unlike Napster, do not require a central server for the free distribution of copyrighted material seem to present a threat to the interests of the content industry's commercial "megaliths" such as Hollywood, the Recording Industry, and so on. Millions of users of peer-to-peer (P2P) computer networks upload their music or any sort of digital files (to an accessible by third parties (equipped with peer-to-peer software) part of their hard drive[7]). Subject to the precondition of having their computers equipped with the same peer-to-peer application, consumers may then exchange their digital files. This, in essence, is a very sophisticated way of

[5] Mark Steffik, ***Shifting the possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing***, Berkeley *Technology Law Journa*l, and Vol. 12:2, available at: http://www.law.berkeley.edu/journals/btlj/articles/vol12/Stefik/html/reader.html.
[6] **See**, for example, **KaZaA**, at: http://www.kazaa.com.
[7] Once one installs a peer-to-peer application, the software creates a "public access" partition in the hard disk drive of computer of the user. Every other user of the application has the same public access point enabled. Once one downloads a song for example, it resides on this part of the hard disk drive. This way, users can swap files with each other.

evading copyright law; users of peer-to-peer networks do not normally pay any compensation to the publishers when they download a music file, software title, or movie to their computer With millions of users logged on to the Internet simultaneously, it is unlikely that a user will not find what he/she is after.

In addition, as bandwidth increases and, particularly, the broadband Internet connections become increasingly popular in Europe, downloading times are much faster than downloading content with dial-up modem connections (most users currently use dial-up modems). This means that, once one switches to a broadband Internet connection, one could download a whole music album in a matter of minutes (in MP3 form). Downloading a whole movie (in compressed video formats so as to save hard disc space and downloading times) could also now be possible at a much faster than normal rate. This, according to the entertainment industry, presents an unprecedented threat to their interests.

The "Napster phenomenon" of the late 1990's could reach up to seventy million simultaneous users sharing, music mainly (MP3) and "pirated" files. Napster was eventually ordered to shut down following a decision of the Seventh Circuit Court of Appeals in the United States of America[8], but the file sharing community has kept growing stronger in sophisticated "cloned" forms such as peer-to-peer network KazaA™. Napster failed mainly because it consisted of a central database where all content was stored. KazaA, on the other hand, only requires users to download a peer-to-peer software program that enables them to create a "public access" point in their hard drive, and to gain access to the public access

[8] ***See***: ***A & M Records, Inc.*** **v** ***Napster, Inc.***, 239 F.3d. 1004 (9th Cir. 2001), *aff'g*, 114 F.Supp.2d 896 (N.D.Cal.2000).

points of the hard drives of other users equipped with the same software. Within the hard drives of users of peer-to-peer networks, there is an extraordinary amount of copyrighted content available for them to exchange. There is no central database thus making it difficult for content owners to sue Shaman Networks, the company that owns KazaA. There are currently dozens of such peer-to-peer applications available on the Internet, making it even harder for the content industries (the music industry in particular) to track infringing behaviour.

It is important at this stage to appreciate there is a fundamental change in the distribution and enjoyment of music, films, and even books. Downloading content from the Internet is an easy and flexible way of enjoying music, films, video games, or anything else that is transferable to intangible (digital) form. Also, a large group of Internet users today is increasingly accustomed to the flexibility of downloading music from the Internet and thus it would be difficult for the entertainment industry to attempt to divert this group of consumers away from this means of distribution and consumption. Essentially, the problem for content owners is that such distribution currently takes place at their own expense. On the other hand, the use of peer-to-peer networks such as KaZaA and the popularity they currently enjoy have increased the awareness of publishers of the market opportunities that are available to them. The major problem is that it is the norm nowadays to download music free of charge. Most, though not all, content that is circulated through peer-to-peer networks is “pirated”. The Music Industry, in particular, is trying to resist and limit the impact that such a radical and powerful cultural (one may argue) movement – such as “file-sharing” – can have

on society. Piracy is the main reason why publishers are sceptical about moving to such a means of distribution as distributing content online.

However, they would have little reason not to do so if they had control over the use of the material in question. Control, for publishers, would possibly mean to wipe the file-sharing habit at least in its current form. Most importantly, publishers would need to control the subsequent uses of their content by consumers following sale, preventing them to make freely available the copyrighted content.

Trusted Computing could help publishers achieve the control that current Internet use makes impossible. It could help content owners to securely publish material online and totally control any subsequent uses thereof.

On the other hand, current rights that consumers enjoy - such as the making of backup copies of one's programs, or printing a legally purchased electronic book (e-book), or making compilations of legally purchased CDs into a writeable or re-writeable disk, and many other legitimate (as the laws of several countries provide) uses could be totally controlled by the content industry. Trusted computing, its programmed **code** that is, could enable **unprecedented control**; it would not just restore the balance but tip it to the publishers' side at the consumers' expense. Trusted computing has been criticised as a platform where publishers can not only protect their rights but also define what their rights should be. The next section will attempt to explain the particulars of trusted computing. Understanding the technology's basic functions is a determining factor on deciding whether trusted computing can enable such control. In this Chapter, it will be shown that control would be possible; however, current technology

(Trusted Computing and Digital Rights Management that is) will not suffice on its own. The technological infrastructure of control is being backed by a corresponding legal infrastructure, as Chapter 2 will make clear in more detail.

1.2. Getting Technical – The Code – The Beginning

1.2. a. Trusted Systems

Mark Steffik, in an important essay in the late 1990's explained how protecting content online could become possible:[9]

> "A trusted system is a system that can be relied on to follow certain rules. In the context of digital works, a trusted system follows rules governing the terms, conditions and fees for using digital works. Suppose that you have a digital work stored on a trusted system, and you do not have a right to copy the work. Then if you ask the trusted system to make a copy, it simply will not do it. Instead, it will give you an error message. If you do have a right to copy and, for example, exercising the right requires paying a fee and certification that you are over 18 years old, then the trusted system would first make sure that the conditions are satisfied. Only then would it make a copy."

Unless a system establishes that it is a trusted system, it will be impossible to carry on a transaction such as buying a digital book. In addition, with regards to downloading music, it means that one should pay a fee before downloading; however, following downloading the music file, the customer could have a very limited scope of uses; some of these uses would be subject to further fees and some would be excluded by content owners altogether. Programming computers

[9] ***Supra*** n. 5

and software in particular ways by adding elements of control to the architecture of personal computing could enable this control.

The success of the above model is subject to the precondition that both customers' and distributors' systems (the computer devices and/or the software applications they run) are trusted systems. Several leading software and hardware manufacturers are already developing digital rights management languages and "trusted" hardware devices. AMD, Hewlett Packard, IBM, Intel and Microsoft, have formed an alliance called the **Trusted Computing Group** (**TCG**). Formerly known as the **Trusted Computing Platform Alliance** (**TCPA**), it now consists of a consortium of companies actively engaged in the computing industry. Initially, their identities were kept secret, but they currently amount to over 200 companies[10]. According to their definition, they promote a standard for a "*more secure PC*[11]". However, as Ross Anderson points out:[12]

"Their definition of security is controversial; machines built according to their specification will be more trustworthy from the point of view of software vendors and the content industry, but will be less trustworthy from the point of view of their owners. In effect, the **TCG** specification will transfer the ultimate control of your PC from you to whoever wrote the software it happens to be running. (Yes even more so than at present.)"

[10] The list of the current members is available at http://www.trustedcomputing.org/tcpaasp4/members.asp.
[11] For more information, visit the Trusted Computing Platform Alliance homepage at: http://www.trustedcomputing.org/home.
[12] See Ross Anderson, ***'Trusted Computing' Frequently Asked Questions***, Version 1.1, August 2003, available at http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html.
[13] ***Supra*** n. 5

To achieve interoperability and security between the different systems (for example, content owners' and consumers' systems) is, in part, intrinsic to the development of public key cryptography technologies. Public key cryptography roughly works as follows:[13]

"In public key systems, there are two keys used by a system for encryption: a public key and a private key. Each computer keeps its private key secret and its public key known. The keys are inverses. Anything encrypted in the public key can be decrypted by the private key. Anything encrypted in the private key can be decrypted by the public key. Assuming that the keys are long enough, decoding a message without having the proper key is very difficult, and it is difficult to derive one key from the other…The consumer system begins by saying the digital equivalent of 'I am a trusted system and here is my certificate.' The certificate itself is encrypted in the private key of a well known digital registry…[T]he distributor system decrypts the certificate and obtains the public key of the consumer's system. Following the 'spy-versus-spy' analogy, the distributor's system has now determined that there is a valid certificate, that it corresponds to a particular consumer system, and that the consumer system has the particular public key."

1.2. b. Digital Rights Languages

Digital Rights Management (the software) defines the rights associated with a digital work. There should be a means of expressing rights and there are various ways that digital rights languages can do that: publishers could attach the rights to the work itself, or store them in a database. Mark Steffik provides an intuitive example of how a digital rights management language could work in practice:[14]

---

[14] ***Ibid***

"…[I]n a typical situation an author would create a digital work using any authoring tool of interest. Digital property rights are neutral to data format and interpretation; that is, they can potentially work with any digital representation of text, pictures, databases, music, or video. Once a work is created, a publisher could import it into a trusted system. He would decide the rights with which to associate the work, and encode them using the rights editor of a publishing program. He could then make the work available on a server for sale online."

Digital rights are for the artist or publisher to define. Consumers have no choice or they might, subject to the condition of paying a fee. This may enable content owners to go significantly beyond what they are entitled by law. For example, there are no safeguards with respect to works that have fallen on the public domain. Content owners may continue charging or conditioning access to such a work when they should not. They may also grant access to a work on the condition that the consumer will not use it for referencing or parodying. There are many possibilities indicating that trusted systems could be a one-sided bargain then. Encouraging such technologies should accordingly involve the building of the necessary safeguards so that certain rights (depending on the jurisdiction) will be respected.

1.2. c. Billing

There is no universal standard as to the form of billing that will be adopted in the context of digital rights management but it is likely some forms will prevail in the future. There is great flexibility, with billing options ranging from online billing to offline billing through the use of PC cards (such as **PCMCIA**™ cards). It is not necessary for the purposes of this essay to explain in detail the types of billing.

However, it is interesting to see examples of how it could work in practice.. Mark Steffik, again, provides a useful guide:[15]

"A work can have different versions of the same kind of right, each with different fees and conditions. For example, a musical work could have a right to play it for a fee charged by the hour. Another right to play that piece may have a fixed fee for unlimited playing. Yet another right to play the piece may give discounts to members of a music buying club. A publisher may give promotional tickets as part of an introductory offer. When a user elects to play the music, he exercises one of the rights matching his sets of licenses and tickets, and his desires, against the various options offered by the publisher."

1.2. d. Copying – Printing – Recording

If a user, subject to paying a fee, makes a copy of a trusted digital work, he can still photocopy it; if he listens to a digital music file, he can still record it to an analogue cassette recorder. In each of these cases, however, the copying is subject to the problem of the degradation of quality of the copied or recorded product. One of the aims of trusted publishing is to prevent the creation of perfect digital copies. On the other hand, it matters not that you might, for example, want to back up your data or that you might copy with a view to a use that falls under the "fair dealing" provisions of the Copyright Act of 1988, for example. Rights are subject to the discretion of content owners. Publishers might grant a backup right

[15] ***Ibid***

subject to a fee, or they might exclude consumers from having such a right altogether.

As previously mentioned, hardware devices could be "trusted" too. Let us now see how control works with respect to, for example, printing:[16]

> "Trusted printers combine four elements: print rights, encrypted on-line distribution, automatic billing for copies, and digital watermarks for making copies that are printed. When assigning rights to a digital work, a publisher uses a digital property rights language to distinguish between viewing (or playing) rights and printing rights...[T]o reduce the risk that a digital copy will be stolen by wiretapping or packet snooping, a trusted system encrypts a document when sending it to a trusted printer…[W]henever the document is printed, the trusted system automatically logs the billing transaction…[F]inally, a trusted printer can mark each copy with watermarks as it is printed. Watermarks can either be highly visible or hidden. They can contain information identifying both the rights holder and also describing the printing event…"

Consumers are not going to be in possession of the data or the devices they will purchase then. Publishers will have complete control over many aspects of "your" computing experience. This is a strong claim that may require further enquiry. The next section examines how trusted computing can facilitate this complete control.

1.3. Current Technology – Surveillance, Control, Censorship, and Resistance

Computer scientist Ross Anderson is a very important source of information with respect to the technology of Trusted Computing. Trusted Computing, according

[16] ***Ibid***
[17] ***Supra*** n. 12

to the Cambridge University scholar, is set to go beyond publishing; it is a platform that, among others, could enable surveillance, censorship, and, control. He describes the basics of current Trusted Computing technology and the **surveillance** and **control** it might enable in the following passage:[17]

"TC provides for a monitoring and reporting component to be mounted in future PCs. The preferred implementation in the first phase of TC emphasised the role of… a smartcard chip or dongle soldered to the motherboard. The current version has five components – the "Fritz"[18] chip, a 'curtained memory' feature in the CPU, a security kernel in the operating system (the 'Nexus' in Microsoft-speak) and a backend infrastructure of online security servers maintained by hardware and software vendors to tie the whole thing together… [The chip] is a passive monitoring component that stores the hash of the machine state on start-up. This hash is computed using details of the hardware (audio card, video card, etc) and the software (O/S, drivers, etc). If the machine ends up in the approved state… [the chip] will make available to the operating system the cryptographic keys needed to decrypt TC applications and data. If it ends up in the wrong state, the hash will be wrong and [the chip] will not release the right key. "

The aim is for these devices and software to make sure that the computer is running the approved software and hardware. Approved software or hardware will be subject to what the entities involved in developing trusted computing consider as such. For example, they might not approve a media-player (a program through which one may listen to music or view a movie on their computer) that is not compliant with their platform of trusted computing. Even worse, publishers might make a product such as a Disney movie, available only

[18] The name is taken from Senator Ernest Fritz Hollings (D-S.C.) who had been a keen proponent of legislation that was in favour of certain segments within the content industry (Hollywood in particular). **See**, ***infra***, Chapter 2 (**2.1.2. CBDTPA**). The first "Fritz" chips were developed as individual integrated circuits that could easily be soldered into computer motherboards. The latest

on the condition that a consumer's system plays it on a particular media-player and no other players such as Microsoft's media-player.

If during the start-up process, the monitoring device finds that a computer runs non-Trusted Computing compliant software or hardware it will not release the cryptographic keys that will make essential content available to the user. This means that - since all programs will have to be certified in order to be operative (this includes software applications and files such as word-processor documents and music files for example) -, consumers would have to comply by running their computer according to the manner imposed by the entities involved in the development of trusted computing technologies. Otherwise, important features of their computers will be disabled.

We should understand trusted computing then, as a platform that not only disables the users' ability to crack the controls imposed by content owners, but one that could go beyond this and significantly control the enjoyment of consumers' computing experience, and, potentially, obscure, influence, and ultimately control their choice of market alternatives. Whereas it might be possible to raise an objection over the legitimacy of such practices (e.g. on unfair competition grounds), it will be difficult to prove that such "locking-consumers-in" practices amount to behaviour that breaches the competition rules - of, for example, the European Union[19] - in the context of such complex technologies.

---

generation of chips will be integrated into the main processors of computers, video-games consoles, mobile telephones, DVD players, *and etcetera*.

[19] "The European Commission has given Microsoft a final opportunity to comment before it concludes its antitrust probe. The Commission has gathered additional evidence from a wide variety of consumers, suppliers and competitors. This evidence confirms and in many respects bolsters the Commission's earlier finding that Microsoft is leveraging its dominant position from

However, this is not all. As Ross Anderson, further notes:[20]

"TC will also make it much harder for you to run unlicensed software… TC will protect application-software registration mechanisms, so that unlicensed software will be locked out of the new ecology. Furthermore, TC apps [applications] will work better with other TC apps, so people will get less value from old non-TC apps (including pirate apps). Also, some TC apps may reject data from old apps whose serial numbers have been blacklisted. If Microsoft believes that your copy of Office is a pirate copy, and your local government moves to TC, then the documents you file with them may be unreadable."

Anderson goes on to say that TC will also make it easier for people to rent software rather than buy it, and if consumers stop paying the rent, then not only does the software stop working but so may the files it created. So if consumers stop paying for upgrades to Media Player, a Microsoft Windows product that Microsoft pre-installs on every new Windows operating system, they may lose access to all the songs they bought using it.

There are more concerns though; trusted computing could support **remote censorship**. As Ross Anderson claims:[21]

"In its simplest form [Trusted Computing], applications may be designed to delete pirated music under remote control. For example, if a protected song is extracted from a hacked TC platform and made available on the Web as an MP3 file, then TC-compliant media

---

the PC into low-end servers and that Microsoft's tying of Windows Media Player to the Windows PC operating system weakens competition on the merits, stifles product innovation, and ultimately reduces consumer choice. The Commission also invites Microsoft to submit its comments on a series of remedies it intends to impose in order to bring the antitrust infringements it has identified to an end. As this **complex investigation** draws to a close, the Commission will continue to ensure a meticulous respect of due process. Therefore, the Commission has addressed to Microsoft a final Statement of Objections." For more information, ***see***, http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/03/1150%7C0%7CRAPID&lg=EN.

[20] ***Supra*** n. 11
[21] ***Ibid***
[22] ***Ibid***

player software may detect it using a watermark, report it, and be instructed remotely to delete it (as well as all other material that came through that platform). This business model, called traitor tracing, has been extensively researched by Microsoft (and others). In general, digital objects created using TC systems remain under control of their creators, rather than under the control of the person who owns the machine on which they happen to be stored (as at present)."

Anderson uses the example of someone who writes a paper that a court decides is defamatory. This person can be compelled to censor it – and the software company that wrote the word processor could be ordered to do the deletion if the defendant refuses. Given such possibilities, Anderson believes that TC could be used to suppress everything from pornography to writings that criticise political leaders.

In essence, the above will enable the Trusted Computing advocates to strengthen their market lead as well, as seen earlier in this section. Ross Anderson focuses on Microsoft™:[22]

" Microsoft, who are now driving TC, were also motivated by the desire to bring entertainment within their empire. But they also stand to win big if TC becomes widespread. There are two reasons. The **first**, and less important, is that they will be able to cut down dramatically on software copying. 'Making the Chinese pay for software' has been a big thing for Bill [he means Bill Gates, founder and owner of the Microsoft Corporation]; with TC, he can tie each PC to its individual licensed copy of Office and Windows, and lock bad copies out of the shiny new TC universe… The **second**, and most important benefit for Microsoft is that TC will dramatically increase the costs of switching away from Microsoft products (such as Office) to rival products (such as OpenOffice). For example, a law firm that wants to change from Office to OpenOffice right now merely has to install the software, train the staff and convert their existing files. In five years' time, once they have received TC-protected documents from perhaps a

thousand different clients, they would have to get permission (in the form of signed digital certificates) from each of these clients in order to migrate their files to a new platform. The law firm will not in practice want to do this, so they will be much more tightly locked in, which will enable Microsoft to hike its prices."

Had one wished to switch to the competition, she would have to face the costs involved in doing so. In "economics language":[23]

"… the value of a software business is about equal to the total costs of its customers switching out to the competition; both are equal to the net present value of future payments from the customers to the software vendor. This means that an incumbent in a maturing market, such as Microsoft with its Office product, can grow faster than the market only if it can find ways to lock in its customers more tightly."

Turning the Trusted Computing controls off on one's computer might be possible though; but there are considerable barriers. Since one's software applications will have to be TC-compliant, subsequent files they have created will be readable, playable, or accessible only if one runs a TC-enabled PC. This means that unless one runs a TC enabled computer, he/she will not be able to read her Word documents, listen to MP3 music files, or view a **DVD** movie. More freedom will mean less choice and in the words of Ross Anderson:[24]

"If the TC apps [applications] are more attractive to most people, or are more profitable to the app vendors, you may end up simply having to use them – just as many people have to use Microsoft Word because all their friends and colleagues send them documents in Microsoft Word. By 2008, you may find that the costs of turning TC off are simply intolerable."

---

[23] ***Ibid***

[24] **See** www.atmel.com/atmel/acrobat/2015s.pdf. Also see Ross Anderson, ***supra*** n. 12.

1.4 Code is the Law – Understanding the Implications for TC

One may recall William Mitchell's contention from the opening of this essay: "***Code is the law***". Trusted computing makes this apparent. The code of Digital Rights Management could defeat the current relatively "anarchic" **code** that allows, for example, piracy to take place today. This might not be entirely true though. Whereas many agree that technological shields of digital assets could be a successful means of regulating access to and use of information (at least, better than current copyright law), it is apparent that each new generation of technologies can be defeated by tools that can be used to overcome or circumvent these controls; but it will take a sophisticated and well-funded hacker to achieve this as trusted computing gets more sophisticated over time.[25] If the hacker succeeds though, nothing stops him/her from publishing the code that cracks the controls of, *e.g.*, a digital rights management language over the Internet. Then anyone can download it and/or install it to their computer and enjoy a vast array of extended uses (that, however, might not necessarily be illegal under current copyright law as the fair dealing provisions of current copyright law might suggest). Publishers are aware of this; it is possible for their fences to be evaded at least, insofar as current technology suggests. This is the reason why they have lobbied hard in American Congress and the European Union over the past few years; the result of their efforts is a body of laws that punishes whoever circumvents code and for whatever reason[26]. It is not the

---

[25] ***Supra*** n. 17
[26] ***See***, infra Chapter 2, DMCA and the EUCD.

creation of code, on its own, that solves the publishers' dilemma. It is the combination of code with harsh laws aiming to protect this code and punish whoever circumvents it that will bring the desired end for the publishers.

On the other hand, Mitchell's contention is really a metaphor. Code is like a kind of a law, because, it defines how we will interact with our computers. Mitchell does not claim that code (a computer program's controls, for example) cannot, or should not be defeated: he merely observes how computers' and computer programs' architecture affects the way we interact with our terminals and with each other.

However, content owners, at least in the context of trusted computing, are set to turn this metaphor into reality. Whereas before it should be understood that the code is like a law, the following equation could change this conventional understanding:

"Code + Law = Code is the Law (at least in a less metaphorical sense**)"**

In essence, once laws support the code writers (or better, the content industry) and punish whoever defeats the controls that the content industry sets - no matter what kind - through a combination of civil and criminal sanctions, code will have a very powerful effect.

The next chapter examines and evaluates the laws in support of code and how they overreach. The focus is on the United States of America and the European Union.

Chapter 2: "The Legal Infrastructure in Support of TC"

2.1. United States of America - The Beginning

2.1. A. The Digital Millennium Copyright Act 1998 (DMCA)

During 1995, Bruce Lehman, the first Patent Office chief in the Clinton Administration in the United States of America, drafted a white paper[27] that was heavily backed by content owners who were sceptical about putting their content in digital form. As mentioned in the previous chapter, digital locks alone can be defeated; content owners, aware of this, have been continuously supporting the enactment of laws that punish those who defeat the digital locks they place on their products.

Furthermore, following the endorsement of the "anti-circumvention" concept in the World Intellectual Property Organisation Copyright Treaty and Performances and Phonograms Treaty in 1996,[28] the **Digital Millennium Copyright Act** (**DMCA**) was passed in 1998 in the United States.[29] The DMCA is now encoded in **Section 1201** of the United States' **Copyright Act**. Here is the core of the Act and the main reason for its controversial nature:[30]

> "No person shall circumvent a technological measure that effectively controls access to a work protected under this title."

---

[27] Information Infrastructure Task Force, Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights, (1995).
[28] **See**, http://www.wipo.int/treaties/ip/wct/index.html.
[29] It was adopted as DMCA's Title I, The WIPO Copyright and Performance and Phonograms Treaties Implementation Act
[30] U.S.C. 1201(a)(1)(A).

Since the enactment of the statute, many have criticised its broad language. Almost all unauthorised decryption of content is banned and subsequent language in Section 1201(b) also prohibits the manufacture, release, and/or sale of products, services, and devices that could crack encryption designed to prevent access to or copying of material unauthorised by the content industry.

In essence, content owners' strategy is to use legislation to bolster technological controls. The DMCA succeeds in doing so by imposing both civil and criminal sanctions for circumventing technological controls. In addition, for the first time, it is not the violation of copyright law *per se* that is the crime; instead, it suffices that one has created the tools that can crack the encryption controls. This is one of the main reasons why the DMCA is such a controversial statute. The next section deals with a few cases that have arisen since the statute's enactment. All of them point to a series of controversies about the rationality, or lack thereof, of the statute's provisions.

Controversial DMCA – Case Study

1) *Universal Studios* v *Reimerdes*[31]

This case concerns one of the most obvious applications of the overreaching nature of the DMCA. It involved the effort of the motion picture industry to limit dissemination over the Internet of **DeCSS**. DeCSS is a software program that disables the Content Scrambling System (CSS) technology that shields Digital Versatile (or Video) Discs (DVDs) from copying. Also, the technology,

[31] 111 F. Supp. 2d 294.

administered by the DVD-Copy Control Association, controlled by Hollywood and several consumer electronics manufacturers, scrambles the content on the DVDs in a manner that results in the discs being impossible to view unless they are played in a DVD-player licensed by the above entities.

At least, that was the case until Jon Johansen, a Norwegian teenager, cracked the encryption code and published the software that cracks it on the Internet as DeCSS. Several websites, including the hacker magazine (a web publication) 2600[32], posted the program and provided links to other websites that had posted it for downloading as well. The Southern District Court of New York banned 2600 magazine from posting or linking to DeCSS code. The Second Circuit Court of Appeals affirmed[33] the decision of the District Court on the 28th of November 2001.

Harvard Law School's criticism[34] on the above case is indicative of the views of a large portion of the American academia towards the DMCA:

> "… [The DMCA imposes] "access controls" and [enforces] "copy controls" that may too easily become limitations on the *use* of copyrighted material."

The reason is that the controls of CSS prevent people who have purchased legitimate copies of discs in DVD format from viewing those products. In the words of the Berkman Centre for Internet Law and Society (Harvard Law School's cyber-law division):[35]

---

[32] http://www.2600.com.
[33] For further information, **see**, http://www.eff.org/Cases/MPAA_DVD_cases/20011128_ny_appeal_decision.pdf.
[34] **See**, http://cyber.harvard.edu/openlaw/DVD.
[35] ***Ibid***

"Without licensed DVD players for Linux [the most important competitor of Microsoft in the operating systems' market] and other operating systems, an entire class of computer users is completely cut off from viewing DVDs. CSS prevents many fair uses of the DVD works even on "supported" systems. DeCSS describes the operation of CSS so as to facilitate the creation of software DVD viewers for Linux and to expand the possible uses of DVDs. Yet rather than welcoming these potential additional viewers, the industry appears to fear that permitting broader interoperability of its format would weaken its monopoly on player devices."

According to the Berkman Centre, the application of the DMCA on the CSS case affects a range of issues that are of fundamental importance concerning progress and individual freedoms:[36]

"We believe that the Digital Millennium Copyright Act's anti-circumvention provisions stifle free speech and competition in the production and dissemination of audiovisual materials. The total access controls imposed by CSS prevent fair use of the materials, hampering our ability to comment, criticize, discuss, or build upon works published on DVD. The injunctions also block First-Amendment-protected expression in and about the DeCSS program and discussion of access control systems."

2) *Felten* v *RIAA*[37]

This case arose when Edward Felten, a computer scientist at Princeton University in the United States, defeated the code for the Secure Digital Music Initiative (SDMI), a copyright protection scheme supported by the Recording Industry Association of America (RIAA). RIAA's lawyers threatened Felten with a

[36] ***Ibid***
[37] http://eff.org/IP/DMCA/Felten_v_RIAA/20020206/eff_felten_pr.html.
[38] For more information, visit, http://www.wired.com/news/technology/0,1282,52665,00.html
.

lawsuit alleging that he would violate the DMCA if he presented his research at a forthcoming academic conference due in April 2001. Professor Felten withdrew from presenting his research; however, the media outcry against the RIAA led it (the RIAA) to say that they never intended to stop Professor Felten from speaking. When the Electronic Frontier Foundation (EFF) sought an injunction against the law, a federal district judge in New Jersey dismissed the case because there was no case or controversy at issue. The United States government had previously stated that scientists attempting to research access control technologies were not subject to the DMCA. RIAA failed on this instance; however, the fact that the content industry has been trying to protect its content at any expense, is becoming increasingly apparent.

3) Copy-Protected Compact Discs (CDs)

As seen earlier, content owners (the Recording Industry in particular) have rightly feared a decline in the sales of music because of the availability of virtually any kind of music over the Internet on peer-to-peer networks. As a result, some studios have introduced compact discs (CDs) that will not play on a computer at all. In essence, code is inserted into the CDs in the manufacturing process; the resulting effect is that the CDs will **only** play on conventional CD players. The motive of the recording industry is obvious: CDs can be converted into MP3s (compressed music files) and then posted to one of the peer-to-peer networks for everyone to download. By disabling the CDs' functionality on a computer, the Recording Industry hopes to cut-down on piracy. Sony has been the pioneer of

this; however, it is very simple to defeat their protection. On the 20th of May 2002, Reuters reported[38]:

> "On Monday, Reuters obtained an ordinary copy of Celine Dion's newest release "A New Day Has Come," which comes embedded with Sony's "Key2Audio" technology. After an initial attempt to play the disc on a PC resulted in failure, the edge of the shiny side of the disc was blackened out with a felt tip marker. The second attempt with the marked-up CD played and copied to the hard drive without a hitch… Internet postings claim that tape or even a sticky note can also be used to cover the security track, typically located on the outer rim of the disc. And there are suggestions that copy protection schemes used by other music labels can also be circumvented in a similar way… Sony's proprietary technology, deployed on many recent releases, works by adding a track to the copy-protected disc that contains bogus data."

The problem with this situation is this: enabling a CD to play on a computer amounts to a breach of law. It does not matter that the motive is to make personal and/or backup copies of the data or to transfer the tracks onto a portable MP3 player. The DMCA is explicit about its intentions: any circumvention of "technological fences" is a felony. This, at least in the United States, is in direct conflict with the notion of fair use, codified in the Copyright Act (**17 U.S.C. 107**). There is a reasonable fear that DRM, Trusted Computing, or any technological fences employed to counter piracy could lead to the demolition of copyright as we have understood it by now. Courts have no choice but to end up privileging the content industries' copyrights over consumers' rights because the law, the DMCA, says so. The DMCA seems to overreach. The balance between private interests and public values in the copyright bargain could end up being displaced (Chapter 3 will focus on this issue in more detail).

4) *US* v *Elcomsoft*[39] (Dmitri Sklyarov)

Adobe[40] currently is one of the leading software vendors worldwide. Its services range across a wide spectrum of products designed to assist in the performance of several computing tasks. One of its most popular products is the Adobe Acrobat Reader. A program integrated within the Acrobat Reader is the e-book reader[41]. The e-book reader's most important characteristic and the main reason why the program is so popular (along with the fact that in its most basic version comes for free) is its user-friendly interface. The program enables viewing of text, pictures, and graphics in the most, up-to-date, elegant and readable form.

Adobe's main aim with respect to the particular product has been to create and dominate a market where book publishers will increasingly publish in digital form. With Acrobat Reader currently being the most popular software application for reading text, Adobe is highly likely to persuade book publishers to publish in digital form; consequentially Adobe will increase its revenues. However, book publishers have been very reluctant in moving into this market. The main reason possibly links to the proliferation of file-sharing servers (such as Napster) or peer-to-peer networks (such as KazaA) and the lessons from the music industry's struggle against those entities. Adobe is aware of this problem though. To this end, Acrobat Reader is designed as a trusted system. Once one purchases an e-book (several publishers already publish in digital form), the purchaser will only

[39] **See**, http://www.eff.org/IP/DMCA/US_v_Elcomsoft.
[40] **See**, http://www.adobe.com.
[41] **See**, http://www.adobe.com/products/ebookreader/main.html
.

enjoy the freedoms that the publisher assigned. For example, the purchaser might be able to copy the whole of the book, or, on the other hand, she might be restricted from doing so altogether. Adobe's product is one of the best examples of the emerging world of digital rights management; it relies on encryption to forbid reading of the e-book on any computer, except on the computer that it is installed and registered. As aforesaid, without such controls, computer users could e-mail the books to friends, relatives, and so on; even worse (at least, from the publishers' perspective) computer users could share the e-books with other computer networks' users over a peer-to-peer network such as KazaA. Adobe's technology was thought to be a guarantee against such copying.

Adobe's e-book protection was not impossible to defeat though. ElcomSoft[42], a company established in 1990 in Moscow, Russia, offered, among other services, a product under the name of Advanced e-Book Processor (AEBPR). In essence, this program defeated the copy-protection features of the Adobe Acrobat e-book Reader. ElcomSoft had reverse engineered Adobe's e-book reader permitting users to decrypt e-books and read them free.

The person mostly credited with hacking Adobe's encryption algorithms was Dmitri Sklyarov, a PhD student at the University of Moscow and employee of Elcomsoft. After having attended a hacker conference in Las Vegas, Nevada, in the United States, Dmitri Sklyarov was arrested by the Federal Bureau of Investigation (FBI) in July 2001. According to the EFF:[43]

[42] **See**, http://www.elcomsoft.com
[43] ***Supra*** n. 37

"[Sklyarov] was invited to give a presentation at the DEF CON conference in Las Vegas about the electronic security research work he has performed as part of his PhD research. His presentation concerned the weaknesses in Adobe's eBook technology software. Dmitry was arrested at his hotel in Las Vegas, on 16 July, [2001,] as he was leaving to return to Russia."

Public outcry from software developers, civil libertarians and people who have generally opposed the DMCA for different reasons led the Department of Justice (D.O.J.) in the United States to drop its charges on the condition that Sklyarov would help them in prosecuting Elcomsoft, his Russian employer.

The trial against ElcomSoft began on December 3, 2002. Although Adobe hired two companies to this end, it could not successfully produce evidence that there were illegal copies of e-Books in circulation because of ElcomSoft's actions. Government prosecutors played an edited videotape of Sklyarov's December 2001 deposition instead of calling him to the stand. Testifying for the defence, however, Sklyarov told the jury that his intent in developing the software was to allow legal owners of e-books to make myriad **fair uses** and to demonstrate security flaws in Adobe's software. On December 17, 2002, the federal jury acquitted ElcomSoft of all criminal charges against it.

Criticising the DMCA

It is hard to say whether, given different circumstances (Sklyarov was a Russian scientist, not an American citizen and the media and the public also was on his side), Sklyarov's defence (the fact that the circumventing technology could have had many fair uses – and not only infringing ones) would be successful. As seen

in the first case study though, it would have been highly unlikely. The law is explicit:[44]

"No person shall circumvent a technological measure that effectively controls access to a work protected under this title."

The law explicitly protects the technological measures (or fences) the content owners set; it protects the code that is:

"Code + Law = Code is the Law"

It does not matter that a circumventing technology can be used for a legitimate purpose, such as a fair use, codified in the Copyright Act at 17 U.S.C. 107. The DMCA implicitly threatens, among others, to eliminate the notion of fair use. The content owners, through the aid of the United States' Code, will exclusively define the consumers' scope of uses. Americans are simply obliged to obey. If not they might face both civil and criminal actions. The above examples show the potential sweeping force that the DMCA might have.

Balancing copyright with other rights has never been an easy task: Yet balance should have been in the minds of the drafters of the DMCA. There is an increasing doubt about whether this has been the case.

According to Siva Vaidhyanathan, a remarkable scholar of copyright and culture, the Clinton Administration's white paper (discussed earlier in the chapter) and the resulting DMCA, signalled the surrender of important safeguards in the United

[44] ***Supra*** n. 30

States' copyright system, at the behest of content industries and with little public discussion. He acknowledges **four** such surrenders[45]:

" **[1]** The surrender of **balance** to control. As a result of the chief piece of legislation in recent years, the Digital Millennium Copyright Act, content providers can set the terms for access to and use of a work. There is no balance if the copyright owner has all the power.

[2] The surrender of **public interest** to private interest. The rhetoric of "intellectual property" in the 1990s was punctuated by appeals to prevent theft and efforts to extend markets. There was little public discussion about copyright as a public good that can encourage a rich public sphere and diverse democratic culture.

[3] The surrender of **republican deliberation within the nation-state** to unelected multilateral nongovernmental bodies. Copyright issues went global. Ancillary markets for music and motion pictures became central to marketing efforts. So the World Intellectual Property Organization and World Trade Organization assumed a greater role in copyright policy as multinational media companies sought global standards that satisfied their ambitions.

[4] The surrender of **culture** to technology. The Digital Millennium Copyright Act forbids any circumvention of electronic locks that regulate access to copyrighted material. Before 1998 copyright was a public bargain between producers and users. It was democratically negotiated, judicially mediated, and often messy and imperfect. Now the very presence of even faulty technology trumps any public interest in fair use and **open access**."

Similarly, according to Lawrence Lessig, the anti-circumvention provision of the DMCA, firstly, should not punish fair uses. According to the Stanford Law School

[45] Siva Vaidhyanathan, ***Copyrights and Copywrongs – The Rise of Intellectual Property and How It Threatens Creativity***, New York University Press, 2001, at p. 159-160.

scholar, the law seems to protect the code more than it protects the underlying copyrighted material. Here is an example of a law that, according to Lawrence Lessig[46], would be less burdensome on consumers of information:

"It would have been simple to construct a circumvention law that was not overbroad in this way. The law, for example, could have made anti-circumvention an aggravating factor in any prosecution for copyright violation. But by protecting the code more than the copyright, the law creates an incentive for…privatized copyright…The law protects, that is, schemes whose ultimate effect may well be to displace the balance that copyright law strikes."

2.1. B. The Consumer Broadband and Digital Television Promotion Act (CBDTPA)

However, the DMCA was not enough. Efforts to create a new "controlled or trusted computing universe" have gone significantly beyond the controversial DMCA, following its enactment in the United States.

During March 2002, Senator Ernest "Fritz" Hollings (D-S.C.), the Senate Commerce Committee Chairman, introduced the **Consumer Broadband and Digital Television Promotion Act** (**CBDTPA**). Formerly known as the **Systems Standards and Certification Act** (**SSSCA**), CBDTPA was supposed to ban the creation of all computer software and hardware that would not be equipped with

[46] Lawrence Lessig, ***The Law of the Horse: What Cyberlaw Might Teach***, Harvard Law Review, Vol. 113:501, 1999, at p. 537.

government mandated Digital Rights Management technologies. The copy-protection standards envisioned by Hollings (acting on behalf of Hollywood, in particular) would mandate the incorporation of what is effectively trusted system architecture, specifying security and interoperability requirements. **S. 2048**'s title, introduced on the 21st of March 2001, read as follows:

"To regulate interstate commerce in certain devices by providing for private sector development of technological protection measures to be implemented and enforced by Federal regulations to protect digital content and promote broadband as well as the transition to digital television, and for other purposes."

The introduction of the bill caused a chain of reactions from literally all directions. Academics, civil liberties groups, technology industry representatives – too many to mention – vehemently opposed the bill. Each group had different reasons; it is interesting and useful, for the purpose of this essay, to see what the implications of a world of mandatory DRM would be for its critics.

Drew Clark provides caustic criticism on the drafters and supporters of **S. 2048:**[47]

" Section 2048 is an extreme example of legislative deference to perceived interests of some copyright holders at the expense of nearly everyone else. It gives the information technology industry and Hollywood one year to create *"security system standards that will provide effective security for copyrighted works."* If they agree, the Federal Communications Commission will implement them; if they do not, the Commission is obliged to attempt to create its own DRM standards. Device manufacturers and software creators who fail to include the mandated standard would be subject to the same criminal penalties as are violators of the DMCA… In other words, beyond simply criminalizing the circumvention of private DRM technologies voluntarily deployed by copyright holders, the Hollings legislation would itself

[47] Adam Tierer and Clyde Wayne Crews JR, ***Copyfights – The Future of Intellectual Property in the Information Age***, Cato Institute, 2002, at p. 152.

mandate the DRM technology to be used, force compliance upon the entire technology industry, and then penalize those who failed to use them as if they had cracked them."

Drew Clark points out that the Walt Disney Corporation had been the driving force in support of the enactment of **S. 2048**, dragging the other five major Hollywood studios along. However, the technology industry had been in strong disagreement with the Bill. According to Clark:[48]

"The debate over the Hollings bill has united the technology, consumer electronics, and Internet rights communities against Hollywood. Among those leading the charge against the bill are the Business Software Alliance, the Computer Systems Policy Project, and the Information Technology Industry Council, all of which represent the biggest players in the software and hardware industries… Many of the same companies, particularly leading lights in the Business Software Alliance such as Microsoft and Adobe, played a key role in lending support to the DMCA."

However, as Clark acknowledges, they now argue against Hollings' bill on a number of different grounds including the following: a) that it presumes bad faith on the part of the technology industry, b) that it gets government involved in the technology standards-setting process, c) that it would mandate a single DRM technology instead of permitting competing ones to flourish, and that by doing so d) it would inevitably freeze technological development.

In short, the above largely indicates a conflict of interests between the Motion Pictures Industry and the information technology industry. Clark goes on to describe what happened when the debate between Hollywood and the Silicon Valley was heating up between officials, during August 2001, at the Progress and

[48] ***Ibid***, at p. 152.

Freedom Foundation conference in Aspen, Colorado, in the United States of America:[49]

"'High-definition recent [movie] releases absolutely must have a secure distribution path to the consumer', said Fritz Attaway, executive vice-president for government relations at the Motion Picture Association of America. 'Unfortunately, some segments of the information technology industry have not reached this conclusion. The information technology industry rebels at the very thought of producing a trusted device' – or a computer with its copying functions disabled – he said. 'I think that is a shame because it is going to drive high-quality content to cable, satellite and other secure distribution systems and away from the Internet.' …Several tech officials snapped right back at Attaway's contention. 'We take a back seat to no one in protecting intellectual property', said Rhett Dawson, president of the Information Technology Industry Council. 'We are committed to protecting your intellectual property, but we are not committed to protecting your business model'

In fact, the technology industry has been developing its own digital rights technologies; it should be borne in mind then that the technology industry is not against DRM or Trusted Computing *per se*. As seen in Chapter 1, several technology "giants", such as Microsoft, Intel and the rest of the participants within the Trusted Computing Group (**TCG**), already try to advance their own business models via the deployment of digital rights management and trusted computing technologies. **S. 2048**, however, seemed to one-sidedly advance the interests of only Hollywood without due consideration of the information technology industry.

The bill eventually **failed**. It remains to be seen whether this would be the case in the near future, should the content and technology industries decide to

[49] ***Ibid***

collaborate in lobbying for a law that would balance between their interests equally.

In a sense that Siva Vaidhyanathan understands[50], copyright seems to lose its familiar grounding over in the United States of America. Recalling his contention earlier in the chapter, copyright today (since the enactment of the DMCA that is) is a one sided bargain, one that is decided at the corporate level; both the DMCA and the failed CBDTPA, have failed to take serious account of the public values. Fair use is one such value, although there are deeper implications with regards to access to information and progress, as Chapter 3 will make apparent in more detail inherent within the copyright bargain. However, this is not an American concern only; the situation is about to change in Europe too. The next section evaluateS the situation from the European Union perspective.

2.2. European Union – Challenges for the Near Future

2.2. A. The Copyright Directive

On the 22nd of May 2001, the European Parliament and the Council of Europe passed a Directive on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society (Directive 2001/29/EC), for Member States to implement into their national laws. Most commonly known as the European Union Copyright Directive (**EUCD**), the Directive allowed a short period of 19 months for implementation by Member States. Greece and Denmark were the only two Member States that met this deadline.

[50] ***Supra*****,** n. 43

The reasons for Member States delaying in implementing the Directive are clear: Following the enactment of the DMCA in 1998, the EUCD, also designed to protect content owners' technological fences, has also been a source of controversy within Europe. That is, the lessons from the DMCA's turbulent passage over the last years have caused scepticism within the European Union's Member States.

Like with the DMCA, the EUCD is the result of the WIPO Copyright Treaty[51] and Performances and Phonograms Treaty[52]. Yet, there are two immediate **policy goals** favoured across the European Union in relation to Internet policy that should reflect on the implementation of the EUCD and that are, in several aspects, different to the policy goals of the DMCA. As the Foundation for Information Policy Research points out:[53]

> "The first is the EU focus on the "**information society**" rather than the "information economy" popular in the US. If this is to mean anything, it is that economic concerns must only be one consideration in government action designed to promote the development of such a society. Other issues such as creativity and a vibrant cultural sphere must also be considered. While strong intellectual property rights are often promoted as a mechanism to encourage and reward creativity, legislation must allow the creative reuse of content that is a vital part of literature, art and other such endeavours. For the great majority of human history, such creativity has flourished without the existence or enforcement of intellectual property rights.

[51] "WIPO Copyright Treaty" (1996). Available at: http://www.wipo.int/treaties/ip/wct/index.html.
[52] "WIPO Performances and Phonograms Treaty" (1996). Available at: http://www.wipo.int/treaties/ip/wppt/index.html.
[53] ***See***, http://www.fipr.org/copyright/guide/

The second is the encouragement of **high-technology research** within the EU, particularly in the area of security."

A more detailed analysis of the Directive, on the other hand, may reveal that it could lead to similar controversies as the DMCA has done in the past. Like with the DMCA, the EUCD's language is on instances broad and vague. As a result, the European Union's Member States should be, at least, cautious in implementing the Directive into their national intellectual property laws. The next section examines the controversies that could rise with respect to the implementation of the EUCD's provisions. Is the EUCD as "trusted-computing-friendly" as the DMCA? Does it, in practice, try to strike a balance between public and private interests or does it contrary to its purpose (stated in **Article 1(1)**) focus on **the information economy** rather than the **information society**?

EUCD – Analysing the Directive

Articles 1-5 – The Basics

As seen in the previous section, the principal aims of the Directive are to:

- **(I)** Bring harmonisation to European copyright law in relation to the fundamental exclusive rights of copyright, as well as the exception to those rights; and
- **(II)** Implement the two WIPO Treaties[54].

Article 1(1) states that:

"This Directive concerns the legal protection of copyright and related rights in the framework of the internal market, with particular **emphasis on the information society**."

Articles 2 – 4 provide for the harmonization of three fundamental exclusive rights, these being the **reproduction right** (**Article 2**), the **communication to the public right** (**Article 3**), and the **distribution right** (**Article 4**).

The **reproduction right**, covered by **Article 2**, is the most fundamental of all copyright exclusive rights. It provides exclusive rights over the reproduction "by any means, in any form, in whole or in part" of "direct or indirect, temporary or permanent" copies of works to performers, phonogram producers, film producers, broadcasting organisations and authors. Several Member States' laws, including the United Kingdom, already provide for this broad reproduction right. However, as Michael Hart points out:[55]

> "…In some Member States there is no express inclusion of temporary copying in their current laws. As digital technology creates numerous copies every time the equipment operates, fears have been expressed that such a broad reproduction right is more akin to a **right to control use** of works **rather** than simply the **copying** of works. Indeed, when the draft WIPO Copyright Treaty proposed a broad reproduction right, the controversy which ensued over the issue of temporary copying led it to being removed from the final Treaty, with all that remained being an agreed statement that 'It is understood that the storage of a protected work in digital form in an electronic medium constitutes a reproduction within the meaning of Article 9 of the Berne Convention'."

Articles 3 and 4 provide for "communication to the public" rights to all of the groups mentioned in **Article 2** (except authors), who are granted distribution rights. **Recital 30** states that all of these rights may be assigned, transferred or licensed. Unlike communication rights, **Recital 28** states that distribution rights

---

[54] ***Supra***, n. 51 and n. 52

[55] Michael Hart, ***The Copyright in the Information Society Directive: An Overview***, E.I.P.R. 2002, 24(2), 58-64, at p. 58.

are “exhausted” by a first sale within the EU. This means that publishers should not prohibit the resale of books; on the other hand, the groups given communication rights may prohibit secondary markets in those works. This, in effect, aims to prevent the resale of their services. **Recital 29** states that rights in services, particularly those supplied on-demand, should not be exhausted by a sale within the EU.

Article 5 provides an extensive list of limitations and exceptions that may be applied to the rights provided in **Articles 2-4**. Any exception outside this list is not allowed, even if it is currently in force within a Member State’s law[56].

Article 5(1) provides for the only mandatory exception within the EUCD: **temporary copying**. However, several qualifications (within **Article 5(1)**) limit the scope of the exception:

> Temporary acts of reproduction referred to in **Article 2**, which are transient or incidental [and] an integral and essential part of a technological process and whose sole purpose is to enable:
>
> (a) a transmission in a network between third parties by an intermediary, or
>
> (b) a lawful use of a work or other subject-matter to be made, and which have no independent economic significance, shall be exempted from the reproduction right provided for in **Article 2**.

The language on the particular section is vague; again, Michael Hart offers some criticism on the broad, vague language of the EUCD:[57]

> “It is by no means clear what ‘an integral and essential part of a technological process’ will be interpreted as excluding. The same uncertainty is also introduced

[56] This is justified by **Recital 31** and **Recital 32**.

by the novel and highly restrictive 'no independent economic significance test', because what copying has no independent economic significance?"

Articles 5(2), **5(3)**, and **5(4)** provide extensive lists of optional exceptions applied to the rights provided by **Articles 2-4**. It is up to Member States which ones to implement.

To further limit the exceptions, **Article 5(5)** provides for the "three-step" test from **Article 9(2)** of the Berne Convention (now incorporated in **Article 10** of the WIPO Copyright Treaty) and **Article 13** of the TRIPS Agreement:

"The exceptions and limitations provided for in paragraphs 1, 2, 3 and 4 shall only be applied in certain [1] **special cases** which do not conflict with a [2] **normal exploitation** of the work or other subject-matter and do not [3] **unreasonably prejudice** the legitimate interests of the rightholder."

Recital 44 also repeats the importance of the three-step test as a limitation to the exceptions, and further provides that:

"When applying the exceptions and limitations provided for in this Directive, they should be exercised in accordance with international obligations."

Following this brief analysis of the first five Articles of the EUCD it remains **unclear** whether the EUCD will succeed in its objective of bringing the laws of the European Union's Member States in conformity. For example, in relation to **Article 5**, the EUCD seems to fail to comprehensively address the exceptions to content owners' rights.

The **most controversial part** of the Directive though, and the one that is of great significance for the purposes of this essay is the one provided by **Article 6**, analysed in the section that follows.

---

[57] ***Supra***, n. 55

Article 6 – Controversies

Like with **section 1201** of the DMCA 1998, **Article 6** of the Copyright Directive has been a great source of controversy within Member States of the European Union.

Article 6 of the Directive deals with the **protection of technological measures** and thereby obliges the Member States to meet the requirements established in **Article 11** of the WIPO Copyright Treaty and **Article18** of the WIPO Performances and Phonograms Treaty. **Recitals 13** and **47** set out the main purpose of **Article 6**. According to **Recital 13** there should be:

> "A common search for, and consistent application at European level of, technical measures to protect works and other subject-matter and to provide the necessary information on rights are essential insofar as the ultimate aim of these measures is to give effect to the principles and guarantees laid down in law."

Recital 47 further provides that:

> "Technological development will allow rightholders to make use of technological measures designed to prevent or restrict acts not authorised by the rightholders of any copyright, rights related to copyright or the *sui generis* right in databases… In order to avoid fragmented legal approaches that could potentially hinder the functioning of the internal market, there is a need to provide for harmonised legal protection against circumvention of effective technological measures and against provision of devices and products or services to this effect."

Article 6(1) provides that Member States must 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 pursues that objective. Essentially, users must know that they are

causing such circumvention; however, the purpose of the circumvention is irrelevant! This is a broad definition that could have a sweeping effect. FIPR states that:[58]

"Even fast-forwarding through a commercial at the start of a DVD could therefore be illegal if restricted by the rightsholder."

The provisions under **Article 6(2)** are similar to the provisions of the DMCA's **section 1201(a)(2)** and **section 1201(b)(1)** encoded in the United States Copyright Act. It requires Member States to outlaw 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 that:

(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.

Again, as with the previous section, the purpose for circumvention is irrelevant. It matters not whether circumvention is done for a non-infringing use. **Recital 49** also provides that Member States may further:

"…[P]rohibit the private possession of devices, products or components for the circumvention of technological measures."

[58] ***Supra***, n. 53

Article 6(3) goes on to clarify the meaning of "technological measures" and whether they are "effective":

"For the purposes of this Directive, the expression 'technological measures' means any technology, device or component…designed to prevent or restrict acts, which are not authorised by the rightholder of any copyright…Technological measures shall be deemed 'effective' where the use of a protected work or other subject matter is controlled by the rightholders 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."

It follows from the above that any technological protection – so long as it falls within the above broad definition – shall gain legal protection against any type of circumvention. Recalling the example of the copy-protected CD, in Chapter 2, drawing on the CD's edge with a marker pen so as to make it playable on one's computer will be illegal under European Union law. Again, it matters not that the user of the "circumventing-tool" (the marker pen) desires to make a, formerly now, legitimate use, such as compiling her CD! The new law is set to exclude such uses from being legally protected. Once the content industry decides to prevent users from certain uses of their legitimately purchased goods, users will have to obey, no matter how unreasonable the demands of the content industry are. The EUCD itself supports the content industry's "fences" and is set to punish anyone who interferes with them.

"Code + European Law = Code is the Law"

One question that may inevitably arise at this stage is whether the European Union's Member States will pass further laws such as the failed CBDTPA,

initiated by Ernest Fritz Hollings in the United States. **Recital 48** is drafted to this end and, essentially, it provides that this is not going to be the case in Europe:

"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."

Recital 48 also states that implementations:

"…should not prohibit those devices or activities which have a commercially significant purpose or use other than to circumvent the technical protection."

It should be noted, at this point, that there is stark contrast between the EUCD and the Computer Programs Directive on the above provision. Computer Software is not as generously protected and **Article 7(1)(c)** of the Computer Programs Directive outlaws any act of putting into circulation, or the possession for commercial purposes of, any means the sole purpose of which is to facilitate the unauthorized removal or circumvention of any technical device, which may have been applied to protect a computer program. It follows that a device that has a dual purpose (one towards the end of a lawful use, the other towards an illegal one) will fall outside this protection. By way of contrast, **Article 6(2)** and **Recital 48** of the EUCD refers to devices or products that have only a limited commercially significant purpose or use other than to circumvent or which are primarily designed to enable or facilitate such circumvention. The potential of the EUCD's overreaching nature is, yet again, not difficult to see.

Here is another controversy of **Article 6** that, according to Michael Hart, has caused fears among consumers' and civil liberties' groups:[59]

"… **Article 6**… could create a technical monopoly over the use of copyright works, lawful as well as unlawful. This is because, if a technical measure is introduced which blocks all copying and it is unlawful to do anything about this, this means not only that rightowners could technically prevent copying permitted by exceptions or where the term of copyright has expired but that, in addition, it would actually be unlawful to do anything about this."

This is also the issue in the United States of America with the DMCA, where the debate is currently heating up not only with respect to the technological protection measures ("fences") of the DMCA affecting the ability of the public to exercise exceptions but also with respect to their **First Amendment** right to **freedom of speech**.

Article 6(4), however, is set to solve the above problem by providing that:

"Notwithstanding the legal protection provided for in paragraph 1, in the absence of voluntary measures taken by rightholders, including agreements between rightholders and other parties concerned, Member States shall take appropriate measures to ensure that rightholders make available to the beneficiary of an exception or limitation provided for in national law in accordance with Article 5(2)(a), (2)(c), (2)(d), (2)(e), (3)(a), (3)(b) or (3)(e) the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned."

FIPR observes a complication with respect to the provisions of **Article 6(4)** though:[60]

[59] ***Supra***, n. 55
[60] ***Supra***, n. 53

"Unlike the DMCA, **Article 6.4** does not give protection to certain groups (such as security researchers) against liability for circumvention offences. In the first instance, it merely requests that rightsholders take voluntary measures to allow the exercise of certain exceptions. **Recital 51** emphasises that these may include "the conclusion and implementation of agreements between rightholders and other parties concerned." … If voluntary measures are not taken, Member States must take "appropriate measures" of their own to ensure that citizens may benefit from the exceptions. However, this is not the case with works made available through on-demand services. Such services are defined very broadly – on "agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them." This definition is also included in **Recitals 25** and **53**."

The language of the Directive, with respect to the definition of "appropriate measures" is, again, vague. For example, will Member States legislate so as to make it mandatory for content owners to design devices to permit exceptions to be exercised by consumers? Or what would happen if they (either the government or the content industry) decided to do nothing about it?

It is hard to come up with any answers yet. It is easy to see that we might end up with imbalanced, one-sided implementations of the EUCD though; Member States may end up favouring, even accidentally, the content industry in an unprecedented manner. That is why they should take extreme caution in implementing the Directive if it is balance what they are after.

Article 7 of the Directive deals with obligations associated with **digital rights management**. **Article 7(1)** (as well as **Recital 56**) requires Member States to provide adequate legal protection against any person who knowingly and without authority performs any 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,

if such person knows, or has reasonable grounds to know, that by so doing he is inducing, enabling, facilitating or concealing an infringement of any copyright or any rights related to copyright as provided by law, or of the *sui generis* right provided for in Chapter III of Directive 96/9/EC.

A distinguishing characteristic of the provision of **Article 7(1)(b)** is that a person must know that she infringes a right. Furthermore, **Recital 57** provides that digital rights management systems should incorporate privacy safeguards in accordance with **Directive 95/ 46/EC** of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data.

2.2. B. The Draft Intellectual Property Rights Enforcement Directive

It seems that the EUCD has not been enough in the context of protecting content owners' intellectual property though. On the 30th of January 2003 the European Commission published a proposal for a Directive of the European Parliament and Council on measures and procedures to ensure the enforcement of Intellectual Property Rights. Of particular interest are the provisions of **Article 21**, which is designed to supplement **Article 6** of the EUCD and would provide protection for

a far broader category of items than either **Article 6** of the EUCD or **section 1201** of the DMCA. According to Gwen Hinze from the Electronic Frontier Foundation (EFF), **Article 21** provides two reasons for concern:[61]

"**First**, it [**Article 21**] would create legal protection for any type of work including or incorporating a "manifestly identifiable" mark or feature. By incorporating such a mark, anyone who wished to do so could potentially assert rights over uncopyrightable works (such as facts), databases, or public domain works… **Second**, **Article 21** would potentially ban a broader category of circumvention devices than that prohibited under **Article 6** of the EUCD or the US DMCA. It would ban "*any technical device which is designed to circumvent a technical device which permits the manufacture of goods infringing industrial property rights…*" If the definition of "technical device" is broad enough to include non-physical incorporated marks such as digital watermarks, then this provision might prohibit the use of any technology or device designed to remove them. **Article 21** contains no provision for exceptions, so the ban would appear to apply even if a consumer's reason for circumvention was lawful."

An extreme example of the over-inclusiveness of the proposed Directive is that devices such as book readers for the blind would become illegal, because they circumvent copy protection by changing the initial format of the product (i.e. an electronic book)! Ultimately, the proposed Directive would succeed in eroding fair use as one of the most important safeguards within the *copyright bargain*, unless there is a specified exception included in the future.

In addition, **Article 21** could mean that the dominant players in the market would have a significant advantage over emerging competitors for the following reason: By prohibiting the sale of compatible, competing technologies they could extend their dominance. **Article 9** has been a source of controversy too. It allows

[61] Gwen Hinze, ***The EUCD and the DMCA in 2003: How Legal Protection for Technological Measures is Shaping Consumers' and Copyright Owners' Digital Rights***, **Up**grade, Vol. IV,

content owners to *subpoena* data on alleged infringers and it could potentially be used to violate consumer privacy rights as well as significantly burden universities, Internet Service Providers (**ISP's**) or any third party intermediaries who must turn students, customers, and *etcetera* in for prosecution!

It remains to be seen whether the Directive will eventually pass and – if so – in what form. Currently, it is largely criticized as a "one-sided" bargain.

So far, the argument has not been against either copyright or taking the necessary steps to protect content owners' legitimate rights. We should desire, if anything, a healthy and balanced intellectual property regime where both public values and private interests are served well. However, current laws seem to go significantly beyond copyright protection. Copyright is being defeated and replaced by a strong private regime of intellectual property protection. It is not the constitution or public-spirited laws that will primarily define how balance should be struck with respect to protecting intellectual property anymore.

Today, "technological fences" offer a private solution, one that is defined by a handful of leading commercial forces. We need, at least, to be suspicious of such regimes. Trusted Computing, in particular, following the analysis in Chapter 1, is not only about protecting PC security and content owners' intellectual property. Trusted Computing can potentially reach significantly beyond these objectives, as we have seen.

We need laws that will safeguard progress not only of the information economy but, most importantly, of the **information society**. Instead, with regards to the

---

No 3, June 2003, available at: http://www.upgrade-cepis.org.

EUCD and the Draft Directive on Intellectual Property Rights Enforcement, we could end up with laws that could have the opposite effect (a sweeping effect with regards to the public interest values. Member States should therefore be cautious in implementing the EUCD and, if possible, they should resist parts of the Draft Directive on Intellectual Property Rights Enforcement too. In addition, with respect to the EUCD, it is hard to see how it, in practice, focuses on the information society for another reason: today, copyrighted works are increasingly made available on contractual terms through shrink-wrap licenses[62] and/or online distribution; it is hard to see how exceptions will be exercised then; consumers are presented with a "take-it-or-leave-it" contract, a bargain that is rather one-sided and leaves little choice to the consumer about exercising his/her rights under copyright law: instead she is bound by a lengthy and complex contract. The rise of private intellectual property regimes could be signalling the end of copyright, as we have known it.

The next chapter focuses on **the values** to be preserved by a balanced intellectual property regime whether it is called copyright or something else. Trusted Computing or any form of private ordering in intellectual property should not be left unchecked by the government in its development. Trusted Computing,

[62]An example of such a license is Microsoft's Windows operating systems. Once one purchases the program, and subsequently runs the disc on their personal computer, they come across a window with a lengthy script. This is the "terms of the agreement". Had they decided to read through the complex script, and had they decided they do not agree with the terms, the program will not be installed on their computer. In essence, users are meant to accept the terms when they break the seal of the box open (following the purchase of the product). Once the seal is broken, the product may not be returned to the retail outlet. Users may not be protected by copyright law; instead, they are bound by the contractual terms of the agreement with Microsoft. Though they can evoke the law of contracts in a subsequent dispute, it seems that they are, technically, forced to waive their copyright-related rights.
.

in particular, could enable unprecedented **control** and the legal infrastructure supporting its development is already in place, as Chapter 2 has made apparent. We need to strengthen the safeguards that will, in effect, monitor the policies employed at the corporate or governmental level and allow interference when public values are being displaced.

Chapter 3: Public Values as a Guarantee for Balance

So far, this essay has concentrated on the concept of the protection of intellectual property (copyright in particular) and the means that have, in recent years, been employed so as to protect intellectual property. The first chapter explored the aspects of the **technology** and how the implementations of technologies such as trusted computing could create imbalances. The second chapter focused on the **law** and how bad laws or bad implementations of laws that seek to support such technologies could further tip the balance in favour of commercial interests. It is desirable that intellectual property should be protected; however, such protection should be balanced. In essence, with regards to the protection of intellectual property, we should desire schemes that will seek the creation or preservation of such a balance. Striking the balance between public and private interests is not an easy task.

Encouraging **values** such as progress and openness are two of the determining factors of the existence of a healthy intellectual property regime. Transparent regulations (something about which the European Union, in particular, is very sensitive), "narrowly-tailored" regulations, and the respect of certain human rights and freedoms – such as the right to privacy – are equally important. Seeking to establish whether the emerging technologies and legal infrastructure respect the above principles is a good guide as to the legitimacy of the current approach to copyright.

The challenge for copyright policy in the 21st century is not merely about copyright's effectiveness (or lack thereof) in the digital age: Most importantly, the challenge is whether the **democratic values** associated with copyright policy should be displaced in favour of strong proprietary intellectual property protection models that narrowly focus on the private interests of content owners. This chapter is dedicated to this end.

3.1. The Copyright Bargain - Progress

Article 1, **§8**, **clause 8** of the copyright and patent clause of the United States' Constitution provides that Congress shall:

"… [P]romote the **progress** of Science and the useful Arts."

In essence, the Framers of the United States' Constitution instructed Congress to create a Statute that would grant for authors, scientists and artists an incentive to create and explore. Without a legal guarantee, safeguarding the making of a profit by those classes of individuals for their work, few would embark on creating, writing and so on. Copyright was not considered to be a natural right by the Framers of the American Constitution though[63]. Copyright, instead, was a statutory creation offering a utilitarian justification of copyrights and patents. Without copyright protection, every publisher would be able to copy any popular work and sell it at a very low price without having to pay any royalties to the author. Ultimately, creativity and progress is what the utilitarian justification of copyright is about as **Article 1**, **§8**, **clause 8** of the United States Constitution

reminds us. This is why copyrights are not perpetual rights (though legislation in western countries has continuously extended the length of copyright terms in recent years): After the lapse of several years a work falls within the public domain. The "property-like" right of authors is limited then; copyright is granted as a limited monopoly, for it is not a perpetual right and at the lapse of the protection-period it becomes non-exclusive.

Trusted computing and **DRM**, on the other hand, are set to defeat the limitations on rights holders' scope of rights. There is no guarantee that a work whose term of protection has lapsed will fall on the public domain by being released from the controlled, "trusted" universe where it will belong in the digital age. There are no guarantees that one may be able to parody, criticize, or freely access a work for academic purposes, for example.[64]

In fact as we have seen in Chapter 1, such private intellectual property schemes will enable content owners to define the rights that will be associated with a work. Whenever someone wanted to make use of a work she should ask the permission of the content owner; if the content owner decided to allow such a use, she would have to pay further fees in order to make such a use. But, such regimes seem to go significantly beyond what is justifiable by copyright. If we decided that copyright is no longer an effective means of encouraging creativity, we should be cautious in choosing what to replace it with. We should certainly be sceptical about a handful of self-interested entities defining our scope of rights,

---

[63] ***See***, H.R. Rep. No. 1494, 52d Cong., 1st sess. 2 (1892), where it is mentioned that in the Constitution's Copyright and Patent Clause, *"There is nothing said about any desire or purpose to secure to the author or inventor his natural right to his property."*

especially when their actions can potentially limit our democratic rights and freedoms.

Assuming our societies' primary purpose, with respect to copyright policy, is progress of the society at large and not merely progress of the content industry we need to safeguard the progress of our societies by helping rights holders protecting their legitimate rights. Instead, current legislation seems to unreasonably place such a duty/privilege at the discretion of the rights holders alone. We need a line of resistance against this; we need safeguards for the preservation of fundamental public values that regulations (whether technological or legal) of this sort may disable. We can do this by setting rules that will explicitly limit the capacity of content owners, or even, governments to displace fundamental values (whether intentionally or not) or limit our freedoms.

Economists may disagree[65] and claim that authors will be persuaded by additional incentives to create more works, or that they might be deterred from creating more works if the bundle of copyrights is not increased, particularly with regards to digital goods.. They may argue for more strict protection at the expense of fair use for example. Relying on pure economic models with respect to copyright though, can be misleading. Copyright is a bargain between the public and the private; it was never intended to be about property or profit in the strict sense (it should be seen as a "property-like" right, a limited monopoly granted by States). Copyright's primary purpose has been the "Progress of

---

[64] See the exemptions under the fair use provisions of the United States Copyright Act, 17 U.S.C. 107.

[65] ***See***, for example, Orin S. Kerr, ***A Lukewarm Defence of the Digital Millennium Copyright Act***, available, in ***Copyfights***, ***supra*** n. 47, at p. 163-170. Also, ***see***, Stan Liebowitz, ***Copyright***

Science and useful Arts" and not the preservation and advancement of the interests of Hollywood and the content industry at large (for these are the major beneficiaries of the current bargain, not the authors or musicians). American policy has changed over the years because the United States has become a "copyright-rich" nation. Hollywood's exports alone amount to billions of United States dollars.

The DMCA and CBDTPA are the result of heavy lobbying from the content industry; so are the forthcoming implementations of the EUCD and the draft IPR Directive in Europe. Protecting the technologies that will protect established economic interests could be seen as another aspect of the nature of the legal infrastructure that is in place in the United States and the European Union, and this is what our societies should resist the most.

3.2. Open Societies

To understand what an open society is about we need look no further than the illiberal autocracies that sprang around the globe during the course of the twentieth century. Soviet Russia was one such example of a non-democratic and illiberal regime. Such illiberal autocracies were closed regimes, places where the ruling "elites" directed ideas, and the expression of ideas. These elites praised on the populations of whole nations for decades, until the end of the cold war at the dawn of the 1990's. Communism had fallen. The United States of America, in

---

in the Post-Napster World: Legal or Market Solutions?, available in ***Copyfights***, ***supra*** n . 47, at p. 197-204.

particular, had been the strongest advocate against the closed, illiberal Soviet-style regimes. As Lawrence Lessig claims:[66]

"We fought this cold war over many generations, for an ideal of the open society. For the ideal that political and social society should be a place where ideas run free, where creativity and progress is not directed from on top, where no one controls your mind. We won that war. The revolutions of 1989 were revolutions in the name of that open society."

According to Lawrence Lessig, most of this rhetoric was, in part, intrinsic to a Jeffersonian belief that nature protected ideas and there was nothing to do to bottle ideas up. In a very much-quoted passage, Thomas Jefferson claimed that:[67]

"If nature has made any one thing less susceptible than all others of exclusive property, it is the action of the thinking power called an idea, which an individual may exclusively possess as long as he keeps it to himself; but the moment it is divulged, it forces itself into the possession of everyone, and the receiver cannot dispossess himself of it. Its peculiar character, too, is that no one possesses the less, because every other possess the whole of it. He who receives an idea from me, receives instruction himself without lessening mine; as he who lites his taper at mine, receives light without darkening me. That ideas should freely flow spread from one to another over the globe, for the moral and mutual instruction of man, and improvement of his condition, seems to have been peculiarly and benevolently **designed by nature**, when she made them, like fire, expansible over all space, without lessening their density at any point, and like the air in which we breathe, move, and have our physical being, incapable of confinement, or exclusive appropriation. Inventions then cannot, in nature, be a subject of property."

There is a connection that can be made here with the previous section. **Openness**, the principle that ideas should freely flow and should be easily

[66] Lawrence Lessig, ***Reclaiming a Commons***,
[67] ***VI Writings of Thomas Jefferson***, 1790-1826, at p. 180-181, H.A. Washington ed., 1854 (letter to Isaac MacPherson, 13th of August 1813).

accessed within a society, is a condition for the ideal of **progress**. Without the former, the latter is impossible. An open society should not attempt to "bottle-up" ideas. Like with most totalitarian regimes, Soviet-communism attempted to create a reality distortion field; information, ideas and so on were channelled through the ruling elites; almost everything was censored; people were silenced. In the end, Soviet-communism failed. The Soviet Union failed because it was not an open society; without openness progress came to a halt. In the end the system collapsed out of exhaustion.

One, however, may not be convinced that the open society has come out triumphant. Enter copyright. The above principles, such as *openness-being-a-condition-for-progress* equally apply to the world of intellectual property protection. If copyright is synonymous with progress, openness is a virtue that is necessary when devising any intellectual property protection regime. It is communism of a sort, one might paradoxically say, though it is "communism" of the good sort. Soviet Russia's channelling, censoring, hiding, controlling information through the ruling elites is the wrong sort; allowing information to be disseminated, for it is not property, ideas are not property, as Jefferson reminds us, is the good sort.

Surely, copyright is in place so as to ensure there are enough incentives for more information and ideas to be disseminated; what copyright should not be about, is for content owners, the modern ruling elites, to control, censor, or unreasonably condition the access of the public to information. This is a Soviet-communist-alike regime, and this is something we should avoid and resist had we desired to

define our societies as open and democratic. Trusted computing, in part, makes it possible for an extraordinary level of control to be exerted upon us. Hence, we need to resist the aspects of technologies (such as Trusted Computing and DRM) that will allow this to happen. Good laws and regulations might help towards this end.

3.3. "Narrowly-Tailored" and Transparent Regulations

3.3. A. "Narrowly-Tailored" Regulations

Lawrence Lessig is concerned with regulations that overreach, regulations that are over-inclusive, that is. As he puts it:[68]

> "For a given objective, there are any number of ways to craft a code solution. Some will be narrower than others. By narrow, I mean less generalizable — these code solutions will solve one problem, but not enable the regulation of many others. And one "constitutional" question is whether there is a value in narrowing the scope of regulation-enabling regulations."

His target is the overbroad anti-circumvention provision of the DMCA. To understand his point he claims that analogously to the picking of the lock of someone's property (such as someone's house or car), the DMCA makes it a

[68] Lawrence Lessig, ***The Law of the Horse – What Cyberlaw Might Teach***, Harvard Law Review, Vol. 113:501, at p. 537

felony to attempt to evade the digital locks that content owners have placed on their digital "property". As we have seen, it matters not that the person who circumvents such technologies might have had no intention to evade the right holder's copyright, such as in the example of Linux users' "cracking" of the CSS code in DVDs so as to make them playable on their computers (installed with a Linux operating system). As Lessig further puts it:[69]

"Yet the anti-circumvention provision punishes a circumvention that simply enables a fair use. The law protects the code, then, more than the law protects the underlying copyrighted material."

The copyright balance is displaced through the combination of technology and over-inclusive laws. Content owners fence copyrighted content and the law provides – what it seems to be as – unconditional support.

"Code + Law = Code is the Law"

On the other hand, some may justify such regulations (the anti-circumvention provisions of the DMCA and the EUCD) as a kind of trespass law. Lessig offers his criticism towards this argument by claiming that:[70]

"Under this conception, anti-circumvention simply protects property owners

from unauthorized access to their property. But the metaphor here is dangerous. If the anti-circumvention provision reached only efforts to hack into a computer system, then "trespass" would be a useful metaphor. But to the extent that the provision aims at rendering intellectual property more like real property by protecting against access to information, rather than against access to computers, then the metaphor of "trespass" is not helpful. **I do not trespass on your idea merely because I think it**."

---

[69] ***Ibid***

As we have seen earlier in the account[71], the solution to the problem of defeating copyrights could be more narrowly tailored by, for example, making circumvention an aggravating factor on prosecutions for copyright violations. Instead, the law has been broadly drafted so as to unreasonably increase content owners' scope of rights.

Narrowly tailoring regulations is a matter of good policy then; it is a value of some sort, one may claim, for it may guarantee that legal rules are equitable; over-inclusive laws may not There is another value though, one that has a more fundamental nature: transparency. The next section aims to outline the importance of transparent rulemaking as well as how the emerging Trusted Computing technological infrastructure might affect transparency.

3.3. A. Transparency

The Draft Constitution of the European Union declares at its preamble that:[72]

> **"**Believing that reunited Europe intends to continue along the path of civilisation, progress and prosperity, for the good of all its inhabitants, including the weakest and most deprived; that it wishes to remain a continent open to culture, learning and social progress; and that it wishes to deepen the democratic and **transparent nature of its public life**, and to strive for peace, justice and solidarity throughout the world."

---

[70] ***Ibid***
[71] ***Supra***, n. 46
[72] ***Treaty Establishing a Constitution for Europe*** (Draft), The European Convention, CONV 850/03, Brussels, 18 July 2003, at p. 3.

Values such as openness and social progress, and the deepening of the democratic and transparent nature of the European Union go hand-in-hand according to the drafters of the Draft European Constitution. Transparency is yet another value and precondition for a healthy democracy as the Draft Constitution reminds us[73] (**Article 49: Transparency of the proceedings of Union Institutions)**. Accordingly, transparent laws and regulations should be an integral part of European democracies. For when regulations are non-transparent, their purpose is hidden that is, a Member State of the European Union, or the European Union itself, will not have acted in accordance to the European Constitution's mandate.

How should we come to understand transparency though? Lawrence Lessig provides us with an illuminating assessment:[74]

"When the state demands that individuals behave in a given way, the individuals recognize that it is the state that is regulating. If they don't like that regulation, they can elect representatives who will repeal it. Regulation is thereby checked by the political process. Transparency, traditionally, has also been a value that constrains the promulgation of regulation…. But what if regulation could be secret — or more precisely, what if the fact that a government was regulating in a certain way could be kept secret? Then this constraint of political accountability would disappear. Because it would be unclear that the source of the regulation is the government, the government could achieve its goal without paying the political price or diminishing the effectiveness of the regulation."

Non-transparent regulations are a very powerful tool according to Lawrence Lessig. He recalls the case of *Rust* v *Sullivan*[75] to explain how it, in practice, has

[73] *See*, ***ibid***, **Article 49: Transparency of the proceedings of Union Institutions**, at p. 40.
[74] ***Supra***, n. 68, at p. 539.
[75] 500 U.S. 173 (1991).

worked in the United States of America. The case involved the Ronald Reagan Administration's opposition to abortion. Because of a precedent set by the case of *Roe* v *Wade*, the government was restricted in the means it could select to deter abortion. The government could have warned, argued, or campaigned against abortion; however, this could have been the maximum allowed by law or the constitution. Instead of doing so, the United States' government devised the following plan: it prohibited doctors in family planning clinics from recommending or discussing abortion as a method of family planning. If asked, doctors where instructed to respond in the following manner:[76]

" [The program does] not consider abortion an appropriate method of family planning and therefore [did] not counsel or refer for abortion."

As Lawrence Lessig argues:[77]

"Now the genius of this method of regulation is that it effectively hides the government's hand… it permits the government to transmit its message without tying the message to the government. Many women are likely to conclude that it is their doctor who is steering them away from abortion — since it is the doctor who is saying or not saying something about abortion. The government achieves its objective by undermining transparency. The success of the program turns upon defeating transparency."

But defeating transparency may, in turn, raise questions over constitutional grounds. On the other hand, the better the government's ability in "hiding its hand", the more likely for government to succeed in preventing questions from being raised, thus making its obligation to make transparent regulations disappear (or, at least, limiting the obligation).

[76] ***Ibid***, at p. 180.
[77] ***Supra***, n. 68, at p.

How may we connect the above with Trusted Computing though? How can regulations be non-transparent in the context of the emerging "fencing technologies"?

It is possible, as we have seen, for government to indirectly regulate so as to achieve a regulatory objective; in the case of the Reagan Administration's opposition to abortion, the government regulated medical practitioners (individuals) so as to achieve its regulatory objective (limiting the amount of abortions). Similarly, a government can regulate through "architecture" so as to achieve hidden regulatory objectives. Lawrence Lessig provides an example of indirect regulation through architectural modification:[78]

> "When Robert Moses built bridges to Long Island that blocked buses, and thereby kept bus riders — and thus the less wealthy [the African-Americans, in particular] — off public beaches, that was a regulation through architecture, and that regulation hid its motives well."

The above example equally applies in the context of the emerging trusted systems technologies. Governments may be able to regulate trusted systems so as to enhance their power in ways non-compliant with constitutional, democratic values. Ross Anderson points out that:[79]

> "Governments will be able to arrange things so that all Word documents created on civil servants' PCs are 'born classified' and cannot be leaked electronically to journalists.

Governments then will be able to regulate behaviour without making it explicit that it is a particular behaviour that is the target of regulation. PCs (and/or the

[78] ***Supra***, n. 68, at p. 540-541.

programs that will be installed in these PCs) could, like with the bridges that blocked buses from bringing African-Americans to the Long Island beaches, be architected (coded) so as to enable governments to non-transparently regulate in the same way. In fact, it is an architectural feature of Trusted Computing to enable such control.

There are multiple scenarios about possibilities for abuse. Regulations through *code* may exacerbate the problem of undermining transparency; for it is easier to hide one's intentions (whether a government, corporation, or an illegitimate venture) through computer code than in the example of the Reagan Administration's indirect regulations of medical practitioners.

Rogue governments, narcotics smugglers, too many to mention, could also benefit from the potentially "non-transparent nature" of trusted computing. Ross Anderson warns us that:[80]

> "Mandatory access control[81] can [also] be useful for smaller organizations with more focused missions: for example, a cocaine smuggling ring can arrange that the spreadsheet with this month's shipment details can be read only by five named PCs, and only until the end of the month. Then the keys used to encrypt it will expire, and the Fritz chips on those five machines will never make them available to anybody at all, ever again."

---

[79] *See* Ross Anderson, ***'Trusted Computing' Frequently Asked Questions***, Version 1.1, August 2003, available at http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html.

[80] ***Ibid***

[81] As Ross Anderson points out: "TC can also be used to implement much stronger access controls on confidential documents. These are already available in a primitive form in Windows Server 2003, under the name of *Enterprise Rights Management* and people are experimenting with them." Though one may imagine the positive role of such a technology with regards to, e.g., national security purposes, it is hard to oversee the potential for abuse.

3.4. The Diminution of Rights and Freedoms

The Right to Read Anonymously – Surveillance - Privacy

Once fully deployed, trusted computing could also enable unprecedented monitoring. For reasons such as the setting of prices efficiently, for example, the content industry will have a strong interest in knowing as much as possible about the habits of the consumers of information. Then it will set its prices accordingly.

The problem with such monitoring is that the architecture of Trusted Computing will enable unprecedented monitoring over what particular individual consumers of information will, for example, read. In the "real world", by way of contrast, it is much harder to track what an individual likes to read. It is possible to know how much information is consumed through the sales of retail outlets. But it is practically impossible on the other hand, to know who exactly is reading/buying what, or how much they do (at least not in as universal a scale as trusted systems will enable). Trusted Computing, on the other hand, will enable such perfect monitoring. Once publishing starts to increasingly take place through the Internet, and increasingly more information products are consumed over the digital medium, it will not be hard to see how surveillance is going to work. Many people are troubled by this aspect of Trusted Computing. Lawrence Lessig asks the following question:[82]

> "Should there be a right against this type of monitoring? In a world where this monitoring could not effectively occur, there was, of course, no such right against it. But now that monitoring can occur, we must ask whether the latent right to read anonymously, given to us before by imperfections in technologies, should be a legally protected right"

Lawrence Lessig believes that, with respect to reading anonymously, there is an ambiguity latent within the American legal tradition. It is not easy to define whether such a right should affirmatively exist, though he seems to acknowledge that there should; it is a matter of *translation* that the judiciary should be called to make.

Others have seen the right to read anonymously as more fundamental. According to Julie Cohen:[83]

> "[Reading anonymously]… is so intimately connected with speech and freedom of thought that the First Amendment should be understood to guarantee such a right."

Then, she goes on to emphasise that:[84]

> "The freedom to read anonymously is just as much a part of our tradition, and the choice of reading materials just as expressive of identity, as the decision to use or withhold one's name."

The problem with content owners' tracking individual behaviour is this: Up to quite recently we had been relatively free from the constraints of perfect monitoring over the consumption of information. In the abstract, monitoring was relatively imperfect. Such control was imperfect because the costs of monitoring were high before Trusted Computing entered the landscape. As Lawrence Lessig puts it:[85]

> "[W]e read anonymously in real space not so much because laws protect that right as because the cost of tracking what we read is so great. When the costs fall,

---

[82] Lawrence Lessig, ***Code and Other Laws of Cyberspace***, Basic Books, 1999, at p. 138.
[83] Julie E. Cohen, ***A Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace***, Connecticut Law Review 28 (1996), at p. 981-982.
[84] ***Ibid***, at p. 1012.
[85] ***Supra***, n. 82, at p. 139.

the liberty is threatened. That threat requires a choice – do we allow the erosion, or do we erect other limits to re-create the original space for liberty?

Article 50[86] of the Draft Constitution for the European Union, on the other hand, outlines the obligation for the protection of personal data. In addition, **Recital 57** of the EUCD provides that digital rights management systems should incorporate privacy safeguards in accordance with **Directive 95/ 46/EC** of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data. It remains to be seen whether such right as the "right" to anonymously read is going to be respected within the European Union.

[86] ***Supra***, n. 68, at p. 40.

Epilogue

"Our Constitution ... is called a democracy because power is in the hands not of a minority but of the greatest number." **Thucydides II, 37** (quoted in the Preamble to the Draft Constitution of the E.U.)

"The fundamental issue is that whoever controls the TC infrastructure will acquire a huge amount of power. Having this single point of control is like making everyone use the same bank, or the same accountant, or the same lawyer. There are many ways in which this power could be abused." **Ross Anderson**

This essay attempted to show that there are different possible avenues for implementations of both the laws and technology related to protecting copyrights that could, in consequence, serve different objectives. The infrastructure (both technological and legal) that is currently being developed, and how positive or negative its effects are going to be for society, will be determined by (**a**) the choices that will be coded within Trusted Computing, (**b**) who will be empowered with making these choices and (**c**) the interpretation and the subsequent implementations of the laws that support it.

This discussion has aimed to stand as another warning sign against the possibility of a world that bad implementations of the technology and law will make possible. In fact, such a world is already becoming reality. There are elements of control built within the technological and legal infrastructure that

need to be reviewed; some should, ultimately, be resisted. The content industry seems to be in charge of the change that is forthcoming with respect to copyright policy, and governments (through laws such as the DMCA or the EUCD) seem to surrender such an important task as the making of copyright policy to the content industry.

Had Thucydides' contention that power should be in the hands of the majority been true, we should be able to, at least, have a saying with regards to such important issues as (**a**) the shaping of copyright policy through the "construction" of the technological infrastructure of Trusted Computing, (**b**) who should, ultimately, be in charge of shaping copyright policy in the 21st century, and (**c**) how much content owners should gain out of the bargain. For, *code* (the architectural principles of computer software and hardware) in the 21st century, will resemble the building of cities:

In essence, we can, for example, shape intellectual property policy (through technology and the rule of law) so as to make it resemble the architecture of medieval cities: freedoms may be limited, public spaces may become extinct, and progress may be narrowly focused on advancing "feudal" interests. On the other hand, we may choose a world where public spaces will be preserved, rights will be enforced, and freedoms will be respected.

Striking a balance has never been an easy task with respect to copyright policy either; we will need to **deliberate** over the choices we will make. *Code*, in turn, will define what type of life we will live in the years to come; for the choices built in computer hardware and software will determine the amount of freedoms and

rights we will be granted, in the context of Trusted Computing and DRM. Hence, we need to know who is in control of the “construction” of this infrastructure, decide whether they are suitable for such a sensitive role, and – ultimately - safeguard that the losses we may have to bear within our societies, are kept to a minimum.

BIBLIOGRAPHY

Anderson, Ross ***'Trusted Computing' Frequently Asked Questions***, Version 1.1, August 2003, available at http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html

Bell, Tom W., ***Fair Use vs. Fared Use - The Impact of Automated Rights Management on Copyright's Fair Use Doctrine***, 76 N. Carolina L. Rev. 557 (1998).

Brin, David, ***The Transparent Society***, Perseus Books, 1998.

Cohen, Julie E., ***A Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace***, Connecticut Law Review 28 (1996).

Hart, Michael, ***The Copyright in the Information Society Directive: An Overview***, E.I.P.R. 2002, 24(2), 58-64.

Hinze, Gwen, ***The EUCD and the DMCA in 2003: How Legal Protection for Technological Measures is Shaping Consumers' and Copyright Owners' Digital Rights***, **Up**grade, Vol. IV, No 3, June 2003, available at: http://www.upgrade-cepis.org

Lessig, Lawrence, ***Code and Other Laws of Cyberspace***, Basic Books, 1999.

Lessig, Lawrence, ***The Future of Ideas***, Vintage Books, 2002

Lessig, Lawrence, ***The Law of the Horse – What Cyberlaw Might Teach***, Harvard Law Review, Vol. 113:501.

Mitchell, William J., ***Space, Place, and the Infobahn - City of Bits***, The MIT Press, 1995.

Shapiro, Andrew L., ***The Control Revolution***, A Century Foundation Book, 1999.

Steffik, Mark, Shifting the possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing, Berkeley Technology Law Journal, and Vol.12: 2.

Thierer, Adam and Crews JR., Clyde Wayne, ***Copyfights – The Future of Intellectual Property in the Information Age***, Cato Institute, 2002.

Treaty Establishing a Constitution for Europe (Draft),The European Convention, CONV 850/03, Brussels, 18 July 2003

Vaidhyanathan, Siva, ***Copyrights and Copywrongs – The Rise of Intellectual Property and How It Threatens Creativity***, New York University Press, 2001.

.