The Family Guide To Digital Freedom

Marco Fioretti

June 29, 2007

Contents

Preface: what is Digital Freedom, and why should I care?

The Family Guide to Digital Freedom explains, in one place and in normal language, what everybody should know about software, digital technologies and digital culture, and above all the **real** reasons why they should care.

Today your rights and the overall quality of your life depend very heavily on which software is being used **around** you: this is true even if you don't care much about computers, or don't use them yet.

Don't be scared! This book is not a software manual, and doesn't require any technical knowledge. If you have ever heard of computers, you have all the background needed to take advantage from this Guide.

Today software and other digital technologies control and influence every aspect of our education, business and social activity. Even if you don't use them personally, you need to be sure they are chosen and used properly, just like the ingredients of the food you order at a restaurant. In other words, you have to make sure that your grocery store, school, post office, government... use *their* computers to *your* best advantage, something that doesn't happen very often yet.

Correct use of software and hardware, together with fair digital copyright laws, can help to protect civil rights, lower expenses for both families and businesses, and help many children to have the best possible education and a good job when they grow up. Properly used and regulated software can help even those who don't use it to keep as much of their money, privacy and freedom as possible.

There's a lot of stuff happening now to make sure that very powerful interests in these fields are protected. This is one of the worst kept secrets of our time, but also one of the best kept. Everything is happening legally, in plain sight, counting on the fact that, until now, almost everybody has been (kept) in such a state of ignorance, disinformation and bliss that one could basically get away with murder. This book is here to change this situation, and allow you to protect yourself and the future of your children.

The real issues are presented mainly, but not exclusively, from a parent's point of view. This book is also written for teachers and other educators, as well as politicians: they all stand to benefit from truly open digital technologies, and each category can and should stimulate the other two to adopt these tools.

Copyright Notice

This book is printed on demand, with as few intermediaries as possible, to be available at the smallest possible cost to the largest possible number of people. Still, almost the whole price of each copy goes to actually manufacturing it.

Illegally copying and redistributing this book, on paper or online, only harms the author, not some faceless, greedy corporation. Photocopying the book (or retyping and printing it) may even cost more in paper, ink, electricity and binding, than actually buying it, if one takes into account the quality of the result and the time spent making copies. The same is true for many other books. Please remember this and help to increase creativity by respecting authors' rights.

Credits

Thanks to Julian and Daniel for their comments and help with proofreading. Any error still present is only my fault.

How to signal errors and send feedback

Feedback about this book is very welcome. Please send questions, comments, critics, error reports, suggestions on how to improve typesetting or any other message to marco@digifreedom.net

Structure of the book

The Family Guide to Digital Freedom describes the fifty most important Things that all parents and educators should know about software, copyright and digital technologies. No previous software knowledge is required. Each Thing has one short chapter devoted entirely to it: all chapters are written in such a way that you can understand most of their content even if you don't read the others, or should you read them in random order.

The subject of each chapter is almost always presented by describing some real world examples and then explaining (when this isn't self-evident) why they highlight a serious problem for parents, students and all other citizens. Of course, reading the whole Guide from cover to cover makes it much easier to see how each issue is related to the others.

The Fifty Things are grouped into four main sections. The first one (Chapters 1 - 3) explains briefly what is really at stake, and why the average person should care at all about it.

The second section (Chapters 4 - 32) describes in detail the Digital Dangers we all face, or are already *bearing* as a consequence of our inattention, and the risks if we continue to do so. Unlike many other books or articles on this topic, we will not deal in detail with technical issues like software performance, reliability or security; don't worry, this is not a software manual or essay.

Instead, we look at how the lack of truly Free (as in Freedom, not price) Information Technology and related laws harms the standard, vital needs of the average family: privacy, culture, education, entertainment, environment, civil rights and security, online information or services and digital communications.

The two following sections explain respectively the real causes of those Digital Dangers (Chapters 33 - 35), and the most effective solutions or errors to avoid (Chapters 36 - 50): what the real problem is, what are the right issues to fight for, and how everybody should do it at home, in the office or when voting or shopping. Some tips on how to live in a world where ignoring computers has already become impossible, are also mentioned.

External and internal cross-references

Throughout this book, both internal and external cross-references are written between square brackets, in bold face. Single numbers are links to other chapters of the book itself. Number pairs, instead, refer to online documents. Therefore, in this example:

```
... scan fingerprint to process payments [6]
... the Winnie the Pooh monopoly [2-1]
```

The first reference points to Chapter 6 of this book (What are Biometrics and RFID). To read the second one, instead, you should visit the Web page http://digifreedom.net/node/83 and click on the first link listed under Chapter 2.

The Digifreedom website

The website associated with the Family Guide to Digital Freedom is http://digifreedom.net. There you will find many more interesting news items and information on these topics than could ever fit in a single book, including tutorials and other services for all new, inexperienced computer users.

The website also hosts forums where all citizens concerned about the attacks on our Digital Freedom can coordinate their efforts to protect it, or simply share their experiences with software and digital technologies.

A Potential Future

Note for the reader

Strictly speaking, the short story which follows is not one of the Fifty Things To Know: it is just an anticipation of what could be the worst effects of the Digital Dangers described in this book. The story was written without external influences, around 1999 or 2000. About one year later I discovered Richard Stallman's Right To Read [**0 - 1**] which deals with the same theme and which you are all invited to read.

A Dinner with The Infoserfs

> Preface: In 2040 society is patronized by benevolent governments closely helped by several monopolistic, insatiable companies. The Internet is not neutral anymore [**9**]. One evening POP Jones, a generic employee, comes back home to have dinner with MOM, housewife, and their teenager son Jimmy. The first thing they hear him saying is...

POP: Hey, we had to lay off computers, today at the office. I hope they'll hire some cheaper humans to replace them. I sure don't want to work without a computer!

MOM: But how would *those* new people work without computers?

POP: Well, they will probably have to .. oh God, this is so humiliating... have to write orders by hand on sheets of paper and ship them inside envelopes as if they were parcels.

MOM: Good heavens, why?

POP: What do you mean, why? Because it's much less expensive, silly! It's much slower, I'll give you that, but in that way we don't have to pay word processing and email licenses. Furthermore, it's much safer and reliable: try to attach a virus or sneak from the network inside a sheet of paper! Oh, and since we are speaking of computers, we can't buy the new washer this month: we have to order the new upgrade of the digital television software.

MOM: What?? But we have just renewed the yearly subscription last month!

POP: Yes, but that was only for basic software license and connection costs. If we don't upgrade we won't see the Superbowl in Tri-di-o-rama next week.

MOM: But we don't need to see it in Tri-di-o-rama. We can see it in the usual VideoBlast format.

POP: No, because they will broadcast it only as Tri-di-o-rama, and we can't watch it with the software we have now, we have to order the new one. You know that the new TVs explode if one tries to put unauthorized software in them [**17**].

MOM: Well, then we won't look at the Superbowl at all. Life is not just football after all.

POP: No comment. Just remember that, in three months from now, they will broadcast everything, including your sitcom, only in this new format. Either we pay now or we don't see anything any more, unless we pay a late fee.

MOM: Wait a moment, did you say Tri-di-o-rama? It's going to be the only format accepted for school projects next year, we have to have it or Jimmy won't be able to graduate! Great. There goes our vacation again!

(enters Jimmy)

JIMMY: Hey, mom I need money!

MOM/POP, YELLING TOGETHER: *AGAIN!?!?* What for?

JIMMY: Can't listen to music I need to hear to write my school essay: you know you gotta pay **every time** you listen to 64 bit quality, don't you? The only way music can be recorded that clear is in MPAA3 format, which is protected with a per-play fee.

POP: You pervert! When I was your age, we didn't need half our parents' income just to listen to some music. And what do you need 64 bits music for anyway? Last time I checked you didn't have 64 bit capable ears, did you? Listen to good old CDs, they're good enough, and free.

JIMMY: Aw, pop, you know they don't make CD players and software anymore...

POP: Never mind then. We can't afford your music. Go to the computer and play some, then, it should keep you out of mischief even better.

MOM: Are you crazy, or what? Do you want me arrested like that other guy for unauthorized music composition?

POP: What?

JIMMY: Yeah, pop, that freak was composing with software he had written himself, and without ever being registered with the mandatory Musicians Association.

POP: Quit with music, then: try smoking, it's less expensive and less dangerous. Speaking of serious matters, have you finally mailed the application form for the InfoAcademy?

JIMMY: Not yet pop, it looks awful difficult, and even damn expensive for that matter.

MOM: But Jimmy: it's certainly expensive, but you know it's the only legal way to be admitted in the journalists guild, and to apply for your very own web site, one on which you can report or write everything you feel even without explicit government approval.

NOTE: this excerpt is available to the public only under the terms of what will be the standard reading license in 2040:

BY LOOKING AT THIS PAGE AND WAKING UP THIS MORNING YOU HAVE ALREADY AGREED THAT:

- *Thou shalt not read this to more than ten people at any given time*

- *Thou shalt not read this more than ten times a month*

- *Thou shalt not read this faster than thirty words per minute*
- *Thou shalt print this only on paper approved by Nocomsoft*
- *Thou shalt ask our permission to tell your friends that you have read this page*

IF YOU ARE SO MEASLY AND ETHICALLY EMPTY TO NOT RELIGIOUSLY FOLLOW THIS AGREEMENT, THOU SHALL DESTROY YOUR COMPUTER IMMEDIATELY, AND PROMISE TO NOT READ ANYTHING AT ALL FOR THREE WEEKS.

Are you laughing? Well, we'll concede that "Infoserfs" is a little bit on the dramatic side, and tends to be pessimistic, but everything you read is what could happen by tolerating laws and practices which **already** exist. The way it could happen, the concrete risks that you and your children would face and the steps to take to make sure that you don't become an Infoserf are described in the rest of the Family Guide To Digital Freedom.

Chapter 1

How much of my life is digital?

What does digital mean?

A digit is a single character in a numbering system [**1 - 1**]. Internally, computers can generate and recognize only two states: presence or absence of a small electric charge. Consequently, they can only represent two digits, 1 or 0, just like humans would be forced to do if they only had one hand with only one finger

Instructions or information are called digital when they are translated into long series of ones and zeroes, that is the only sequences of digits that a computer can understand, store and process.

If the story ended here, it would be mere technology, and most people could just stop reading this book and forget about the whole thing. The revolutionary and dangerous part of the story is the fact that today practically everything can already be expressed in digital format: music, banking transactions, movies, Census records, computer programs, Social Security numbers, whole books, fingerprints [**6**]...

This has already started to turn **your** whole life upside down for two reasons. If every service or information is represented in the same way (long sequences of digits, called *files*) everything can be also *stored or transmitted* in the same way.

This is a much, much bigger deal than it would seem at first glance. Just a few years ago, preserving or sending a friend **exact** copies of one's letters, music in vinyl albums, pictures or "devices to create neat printed reports" was still a real hassle, and a really expensive one too. One would have to photocopy or rewrite all the letters, buy other albums, order reprints of all pictures and buy another *typewriter*. Vinyl albums couldn't store pictures and camera films couldn't store songs.

Today, if both you and your friend own a computer, you just have to copy all your letter *files*, your music *files*, your pictures *files* and the *files* constituting your word processing program onto one CD: since all those things are digital, they can be stored in the same way. With a fast Internet connection the CD isn't even needed: since digits are represented with electric charges, they can directly travel along wires or radio channels.

The other reason why digital technology is a real (sometimes dangerous) revolution is, again, that the digits 1 and 0 correspond to presence or absence of a small electric charge. The world is absurdly full of such charges, and they are all exactly equal to each other: a digital "object" can be copied endless times, and each copy will be just as good and as original as the first one. This applies also to **false** documents, of course.

This is the main reason why this book is so important: since almost everything you do can be digitized and whatever is digital is generated, distributed or controlled through software, it is very dangerous to ignore how software and digital information is created and controlled.

So, how much of my own life is digital?

It turns out that a lot of your life is already digital or digitally managed, even if you never use a computer. Some things are (at least apparently) controlled by you, some by others, but there are dangers in both cases. Here are some examples.

Do I still own my own memories and feelings?

Today, thanks to computers, many of us can save, enjoy and share much more of our lives and much more easily, than our parents and grandparents could. Sometimes this already happens online with picture galleries [**1 - 2**], social bookmarking [**1 - 3**] or online diaries.

The truth is that all this, unless it's done in the right way, is a very fragile illusion, and isn't even yours. Let's assume that you finally find in your attic, at the bottom of that big trunk, the original floppy disks of your PhD thesis written no more than ten years ago, and you want to print them again for old times sake. Can you? Very probably not. Do you at least know why [**40**]?

Many of us still have handwritten letters or old photographs from grandparents or from their own infancy. It is really easy, albeit time-consuming, to create digital copies with a computer and a scanner, but such copies may last much less longer than the originals: viruses, scratched CD-roms not usable anymore, computer crashes, incompatibility with next year's DVD player or software... Do you want to cope with this? Can you really call this progress?

What if you cannot use your pictures or certificates because the software to display them has disappeared? They're not yours then, nor is your life. The same applies to anything that you stored digitally with a secret code whose key is only known by somebody else [**40**], something that still happens with most office documents.

Sadly, all this also happens in the academic world, which at least ideally should be fighting to the death any attempt to destroy and forget information. Just a few years ago, technical papers and theses were almost always available in top quality digital formats that everybody could read from almost any computing environment [**35**]. Today, you often have to have the same presentation or word processing software of your professor, or just resort to photocopies. The same applies to availability of course material online, e-learning [**1 - 4**] and such.

It’s not just your diary, it’s your peace of mind

You might just conclude that all this is not such a big deal and forget the whole thing, but that would be a big mistake.

What if you are being audited by the Tax Office and the vanished files contained tax relevant information, for example? Think when the same thing happens to all the other official documents that define your and your children’s life. School and medical records, property certificates, pension payments, law texts, contracts, SAT procedures: all these things have already been digitized, or will be as soon as possible because it is so much easier and economical, for the reasons explained at the beginning of this chapter.

This is the first thing to know: your life **is** getting more and more digital every day, whether you are still a toddler or have already retired to some tropical island. As with any other really great thing, it can be very good or very bad. While there is no need to become a programmer, it is essential to understand how this happens, and how it must work to **your** advantage.

Chapter 2

Who owns information, ideas and fun?

Copyright is the legal right to control or prevent, within certain bounds and for a limited period of time, the distribution of creative works. Copyright can be a great incentive for authors, the fairest way to reward them and, eventually, a great advantage for society as a whole. Unfortunately, without most people realizing it, today copyright is being pushed to ridiculous extremes that must be stopped as soon as possible because they can directly harm any of us by messing with our money and private lives. Here are some examples.

The bear who keeps Justices busy

The Winnie the Pooh books were written about *eighty* years ago, from 1924 to 1928. Their author, A. A. Milne, died in 1956, that is *fifty* years ago. But Justices and employees paid with public money, all the way up to the Supreme Court of the United States, have been engaged for *twelve* years looking at lawyers debating which other people, who weren't alive back then and *never wrote a single word of those books*, should still have a monopoly on the money made through Winnie the Pooh merchandising [**2 - 1**].

The cruelest dinosaur who ever lived

You can joke about your President, but not about an imaginary purple dinosaur. Seriously now: don't you or your kids dare put online a parody of Barney, if you want to avoid an extremely real lawsuit from what has been defined as "baseless legal threats" [**2 - 2**] and a "prehistoric understanding of copyright and trademark laws" [**2 - 3**]. As we write, the lawsuit is still ongoing. The same thing, of course, could happen with any other cartoon or comics character, of course.

Avada Kedavra: the fan killing curse

Some years ago, some teenagers used to meet on a website to share their own Harry Potter stories: not for profit, mind you, just to practice and improve their writing skills. The Warner Brothers company sent out cease-and-desist letters [**2 - 4**], to defend their frail finances from such deadly attacks. Eventually they had to give up, but only after a lot of unnecessary, potentially very expensive legal troubles for the families of the girls and boys involved.

All YOU need is love: hand your money over, please!

Today, many parents and grandparents would probably like to buy, now that they have enough time and/or money to enjoy it, the complete works of the Beatles or some other famous bands which one cannot enjoy anymore in live performance. The Beatles, for example, broke up in 1970, when they (and their recording company, agents and so on) had already made more than enough money to live comfortably. Ideally, today you could buy all their all recordings, including those which were never released as albums or went out of circulation shortly after release.

Unfortunately, this is either impossible or at least as expensive as when the music was first released, because, after more than forty years, those recordings are still under a monopoly. In 1977, scientists could not let aliens know about the Beatles, by sending samples on their music on the Voyager spacecraft, for fear of being sued [**2 - 5**]. Even if all four Beatles had approved the idea. Copyright of the *first* Beatles album will expire (if laws don't change again) only in 2013. Without such a long copyright, everybody could already repackage, sell or distribute online the original recordings; that would be a great advantage for all fans and lots of job opportunities, all without doing any real damage to the *creators* of that music. But no, most of those songs now "belong", as far as distribution is concerned, to Michael Jackson [**2 - 6**] who didn't write them and doesn't exactly need that money to survive.

Copyright extension beyond any reasonable limit harms all creative activities, not just music. Italian playwrite and philosopher Luigi Pirandello, Nobel Prize winner for Literature in 1934, died in 1936. Italian theater companies continued to pay royalties every time they performed his plays, according to copyright law, for *seventy* years after his death.

In 2006, however, as soon as that term expired, royalty payments on Pirandello's works were extended with a legal trick until 2013 [**2 - 7**]. In other words, the incentives for actors and theater managers to keep Pirandello's work alive have been artificially limited for seven more years, probably *lowering* the residual economic value and benefit of those plays.

Asking permission for your own home movies

There's nothing bad in adding some short clips or songs from commercial movies in **your** home movies, right? Wrong! In the United Kingdom, according to the 1988 Copyright, Designs and Patents Act, copyright is infringed also when storing the copyrighted material in electronic format, even if it is only for private usage. In plain English: the police *can* go after you if you make a backup copy of your regularly purchased videotapes or if you mix clips from a TV movie or talk show to your private holiday film.

At the end of 2006 the Gowers Review [**2 - 8**], a study on how to modernize these parts of UK law, included recommendations that private copying is allowed, but this doesn't guarantee that such exceptions will find a place in future laws. Several other countries have laws similar to the current one in UK: is essential to act soon, in every country, to guarantee that the situation doesn't get worse.

In the meantime, those who asked for permission to include copyrighted material in their own home movies found out that even an absolutely *private and non-commercial usage* is either completely forbidden or priced up to 900 USD dollars for a 15 second clip [**2 - 9**]. Of course, you may rely on the fact that the police (and the movie studios) have more urgent things to do than getting authorizations to check your home movies. The fact remains, however: even ignoring the damage made to society as a whole [**15**], you **can**, and will, be sued if you violate these rules and the police find out for any reason.

Is this justified?

What is life like under the current regime? Let's summarize:

- purely artificial barriers often make it impossible to legally find or buy music that we loved when we were younger. It is also impossible to enjoy many old documentaries and old movies because nobody keeps them available at a fair price
- it is illegal to spice up our own, private home movies with what we prefer
- today's children *must* use the Internet (consumerism always finds new targets) but cannot use it to share *their* stories, or make innocent fun of their heroes

All these absurd but true little stories are just a small part, the easier part to understand, of a titanic battle which is happening right now, one that can seriously screw up your and your children's lives. There is much more at stake, however.

Our children are not losing just the freedoms that we all enjoyed. Many old movies or TV news shows have not been preserved properly by their producers and are still available only thanks to crimes, that is illegal copies. Today, for the first time in human history, we have the technological capability to record and pass on to future generations almost everything *we* (not some movie company or its sponsors) consider valuable, and to preserve it from loss and corruption as long as we want.We can't leave all this to the mercy of the limited resources and changing business strategies of any company or group of companies.

Chapter 3

How much do we all pay for software?

The answer to this question is very simple: an awful lot, even if not all of it, nor its bigger part, it's money and if we don't use computers.

As far as we are concerned, the word "software" [**3 - 1**] refers to any sequence of computer instructions which is coded in digits [**1**] and stored inside some electronic device. A single piece of software constituted of one coherent sequence of commands, all linked to each other and designed to perform a specific task (writing text, processing images, playing digital music...) is usually called a *software program.* Each software program is specialized and, for a lot of reasons which will become clear later, different programs born to do the same job are frequently incompatible with each other.

What if (following the advice in this book [**40**]) software programs became something that can be easily replaced without disrupting business, just like pens or paper? What if it were much easier than today to have software support or customization from many different and completely independent contractors, switching from one to another when the service is better?

The expenses to buy new software licenses [**36**] and new computers every few years could be sensibly reduced, with beneficial effects for Schools, Public Administrations and businesses of all kinds and sizes, especially medium and small ones. In an ideal world, some of those savings may even end up in your paycheck or, why not, your tax bill or any stocks you might own.

What is actually happening, instead, is that many of the companies from which we buy goods or services are still forced to spend more than they could on their computers, making **our** bills heavier. This happens all the time, and it only takes a bit of attention to see it. Here are two of the most common examples.

The overcomputing teller

Just about everybody who enters a bank (or any other public or private service agency: real estate, insurance...) complains about all the fees popping out of nowhere which, we are told, are spent on improving customer services, to save us time and hassles and so on. So far, so good.

The next time you go to your bank or any public office, please have a look at the teller or employee desk. Very often, especially in banks, it will be a very cramped quarter in which computer, keyboard and monitor barely fit (never mind the poor employee). Nine out of ten times, there will be some labels on the computer case, declaring that the box was designed for the best operating system on the market, with some top notch processor inside.

For the record, processors are the central integrated circuits in each computer, the ones which run the software and control all the other hardware. An operating system, instead, is the base set of softtware components that make it possible to start up a computer and interact with it at the lowest level. It is the operating system that starts and allows to work all these programs humans actually use to do useful or funny things.

Great, isn't it? Bank tellers, however, only have to deal with a few standard procedures. This is why, almost always, their screen will either be filled by only one, very ancient looking, character window or a Web browser, an environment in which a computer mouse would be useless or slower to use than the keyboard alone.

In both cases, the real work happens on some very powerful but remote computer: what you see besides the teller is very little more than a keyboard and a monitor with a very long extension cord. Even very old or limited computers would be enough for that.

Did grandma's plane land or what?

You are at the airport, waiting for some relative to land, when all of a sudden the monitor listing all incoming flights goes crazy, filling itself with small boxes and tiny error sequences. Did it ever happen to you? This accident is so common that there even is an online picture gallery entirely devoted to it [**3 - 2**].

Another gallery [**3 - 3**] shows the same thing happening on many other devices you use every day, including a McDonald's drive-thru [**3 - 4**]. Very often what is happening is the same thing as in the previous example: somebody bought general purpose, unnecessarily expensive computers and software to display a few lines of static text. But it's no problem, is it? After all, it's passengers who pay for it, and who cares about reliable airplane schedules anyway?

Don't let this pass

If expensive computers are purchased (with your money!) in cases like this, it may be because somebody was fooled by some colorful brochure saying "Nothing free is valuable, our software is the most expensive so it must be the best, too bad it runs only on the newest computers, just pay". In short, the next time check and require that they explain to you just how much of your fees comes from this attitude. Remember that the same kind of tax is hidden in almost every service you use [**3 - 3**]: driver's licenses, insurances, birth certificates, schools, parcel services... if it's done using software, it is likely costing more than it could. Luckily, better solutions, feasible in many real world cases are already available [**38**].

How can this be possible?

What exactly is it that makes it possible for software to remain more expensive than hardware, and much less open to free competition? Why can't we (or our governments...) shop for cheaper computers and programs just like we already do with clothes, groceries and screwdrivers? The answer is that all those goods and their providers have no "history": they don't remember where they came from, and the same happens with what we do *with* those goods. A screwdriver will work no matter where the screws were bought. If you stop going to the same grocery store where you shopped for ten years because a cheaper one opened around the corner, the food you bought at the old place is still edible, and can be mixed with the one you'll buy next week.

Software instead, if chosen and used improperly, is just like nuclear power plants, which remain dangerous even after you've stopped using them. A school can change its paper provider without any compatibility problems, but if it changed computer software without thinking and planning very carefully for it, it would stop working literally overnight. In addition to that, bad software is dangerous also because it can force **others** to use and pay for it even when they would prefer another program.

The exact reasons why this happens are explained, together with the solutions in another section of the book [**40**]. For now, it is enough to remember that software, unlike most other goods and services that everybody must use, has much more power to perpetuate and impose itself, and this is the reason why it is so abused and expensive.

Chapter 4

Are our governments spying on us? How much?

It depends on what you mean by spying. Governments have always had, for example, the possibility of intercepting traditional phone calls. There are even official specifications like, in the USA, CALEA *(Communications Assistance for Law Enforcement Act)* which define the technical requirements that any telecom equipment **must** satisfy to make wiretapping possible. Recently, there have also been requests to do the same with phone calls made over the Internet [**32**], but there's more to worry about.

Echelon and friends

In the late 1990s, a system called "Echelon", used by several secret agencies, caused quite a stir in hi-tech circles. The purpose of Echelon was mass eavesdropping on communications worldwide. Some people also floated the hypothesis that Echelon was used for *economic* espionage to the advantage of USA corporations. As of the late 1990s/early 2000s, Echelon intercepted telephone calls and other communications on satellite links and transoceanic cables. The best source of information about it are two reports, of which one is available online [**4 - 1**], commissioned by the European Parliament.

Whatever its actual power is or was, Echelon is simply one network and one of the possible methods for mass interception. There are plenty of other countries that perform, or have evaluated, the same activities. Regardless of the country, today there is also a strong push to monitor all communications in the same way. Technology is only making it harder to resist to this temptation. In June 2006, for example, the F.B.I dropped demands for Library Patron Records [**4 - 2**] only after a long legal battle.

Both individuals and businesses are exposed in the same way. The Society for Worldwide Interbank Financial Telecommunications (Swift) maintains a common database of billions of financial transactions in 200 countries. The USA Treasury Department had unlimited access to that database for several years after 2001 [**4 - 3**], before Swift was able to restrict their operations, leading to official complaints from the European Community [**4 - 4**].

A law proposed in USA in February 2007 demands that all Internet service providers track their customers' online activities just to aid police in future investigations [**4 - 5**]. Similar laws already exist or are under discussion in most other countries. A wiretapping program proposed in Sweden in March 2007 [**4 - 6**], for example, would enable the interception of "millions of telephone calls, email and text messages". Another bill in the United Kingdom [**4 - 7**] would allow both widespread data sharing and comparisons between public and private databases and the range of purposes for which these analyses can be carried out.

Digital mines

Data mining is the activity of analyzing huge quantities of digital data to discover which ones are related, how and why. Corporations and Government Agencies routinely perform data mining, in order to discover consumer habits and terrorist activities.

The Narus software company makes a traffic analysis software able to intercept all e-mail messages (complete with attachments), see what web pages are visited and reconstruct phone calls made through the Internet. There have been rumors of Narus being installed inside several switching offices of the AT&T phone company

[**4 - 8**].

One may believe that, since the amount of textual information flowing across the Internet in any second is really huge and constantly growing, the probability of being personally watched through data mining is almost non-existent, but this could become an illusion pretty quickly. It is true that Internet traffic is growing so fast that no software program, no matter how fast, could keep pace with it: at least another company, however, goes one step further than Narus to solve this problem. Exegy sells a small specialized integrated circuit, called the TextMiner [**4 - 9**]. Once it's mounted on a small computer extension board, the TextMiner is capable of scanning in real time up to one billion characters per second, to find, up to 260 times faster than any normal computer, specific words or phone numbers in a data stream.

Is it legal to protect personal information?

It is possible, in order to keep private any personal files you may have on your computer, to digitally encode them. In some countries, however, you could already be prosecuted if you don't renounce this protection when the Police "ask" you to do so [**4 - 10**].

In England, for example, the possibility for the Police to demand decryption is part of the Regulation of Investigatory Powers Act (RIPA) since year 2000. If some conditions are met, Part III of RIPA makes it a serious offense not to let them read your encrypted files. The reason is to force potential criminals to hand over **all** the proofs of crimes contained in their computers, even if they were encrypted.

For exactly the same reason, however, RIPA has already been described as a "hair-raising" piece of legislation by people thinking about the effect the powers being given to police would have: *"you do not secure the liberty of our country and value of our democracy by undermining them,"* Lord Phillips of Sudbury said. *"That's the road to hell."* Professor D. Korff [**4 - 11**], a Dutch human rights lawyer and data protection expert, said there was a real question as to *"whether the powers undermined the presumption of innocence* *that human rights legislation enshrines".*

Even looking at the issue from a purely technical point of view, experts point out that it may also be possible to claim that one's computer was under someone else's control, making the usefulness of such powers pretty doubtful. Of course, if Trusted Computing [**17**] became ubiquitous, such assertions may become unsustainable in Court.

What should you do?

All this must not stop people taking care of their own digital files, especially now that we store in personal computers, including laptops which are very easily stolen, so many private and business data [**22**]. Digital cryptography is the technique of translating any block of bits (from your credit card number to each email message or document in your computer) in another block of bits that can be translated back only by somebody who knows the key to reverse the translation. If you use a computer, please start encrypting everything you can. The real solution to prevent potential abuses is to use the right technology in the right way, fix broken laws through your vote, activism and so on, and immediately denounce the same abuses when they happen, maybe through the website associated with this book.

Chapter 5

Do we still have some privacy?

Back in 1999 the Chief Executive Officer of Sun, a company which makes many of the computers used to store or route public records or credit card transactions, was already saying ”You have zero privacy anyway - get over it” [**5 - 1**].

The way governments use or abuse digital technology to mess with our privacy has already been discussed in the previous chapter [**4**]. Let’s then go through a quick review, thanks to some examples, of how other *individuals* can do the same, **even** if we don’t use a computer, and what this really means.

The official customers policy of Toysmart.com was to never share customer data with any third party, but in mid-2000 they were caught while selling the e-mail and mailing addresses and shopping histories of 250,000 customers [**5 - 2**].

During a 2004 interview Steven Rambam, a private investigator, showed that he had been able to discover the Social Security number, address and other personal data of his interviewer in the previous 24 hours [**5 - 3**].

In July 2006 Internet Service Provider America Online placed on a public website the most recent Internet searches performed by more than 650,000 of its customers [**5 - 4**]. The reason was to make those data available to Internet usage researchers. The published files did not contain the real names of those people, but were complete enough to make it possible to identify at least two of them. Consequently, several civil rights groups filed complaints with the USA Federal Trade Commission, but the damage had already been done.

The danger doesn't only come from businesses. Even other individuals can seriously damage your privacy and reputation. Image search engine Polar Rose is developing a software that, when ready, will allow users to enter the identity [**5 - 5**] of *any* face they recognize in online images (even without the consent of the owner of that face) into a central database. Everybody will then be able to search in that database all the online images which contain a given face.

In the meantime, it is already possible to get in trouble even without recurring to such sophisticated technologies. When two San Antonio students published an obscene web page in their administrator's name [**5 - 6**], the result was a lawsuit against both the students and their parents, considering them guilty for not supervising their children's activities online.

Of course, stupidity isn't restricted to a single age range. During the summer of 2006, a 30 year old guy posted an online adult ad, pretending to be a woman, just to publish on the Internet all the pictures and messages he received in answer [**5 - 7**]. Just for fun, of course.

Browsing the Internet like an elephant

The default (and for most people, the only) way to surf the net is still to leave a more or less signed track wider than an elephant herd. For example, the online portals of many newspaper and magazine use the same service to generate printable versions of their pages. In those cases, whenever one clicks on the "Print This" button he or she is redirected to a central site, different from the one originally visited, which handles the printing service for third parties. In this way, one site, always the same one, gets a detailed picture of what you consider worthwhile enough to print, even if you only visit websites which apparently are totally unrelated to each other. More information is available on the Digifreedom website.

Tattletale electronics

Sometimes the privacy attack is just embedded in the newest and most popular consumer devices. According to some reports, the maker of the famous Photoshop software, Adobe, is developing tools which will be able to match a digital photograph to the individual camera that shot it [**5 - 8**]. Even selling your old cell phone can be a serious attack on your privacy [**5 - 9**]: when some security expert, in August 2006, purchased ten used cell phones for a test, they found all kind of sensitive data on them, from passwords for bank accounts to prescription details which the previous owners had not erased correctly, when they *had* bothered to perform the proper procedure.

What about the dear old photocopiers used for everything from tax returns to insurance claims? Most models manufactured in the past five years "temporarily" store images on internal disk drives which in practice are almost never erased. Sometimes the photocopiers are sold with many of the copies they made still stored on the drive. The problem is so serious that in March 2007, just ahead of tax time, the Sharp Document Solutions Company had to issue a public warning about this risk [**5 - 10**].

The final lesson is the same in all cases: anything about you that you or anybody else divulges online or stores on some electronic device *"can come back to haunt you, even when divulging that information is illegal"*.

Can your files die with you?

Another, completely new category of privacy-related problems has just started to surface: what happens when somebody dies and his or her will, bank account number, letters, pending payments and so on are stored in a computer, whose password nobody knows anymore? What if that computer doesn't even belong to the person who passed away [**28**]? What happens if the password was a biometric one [**6**]? How can the relatives use it, assuming it wasn't destroyed with the rest of the body in a car accident or fire?

This is not some hypothetical future scenario: when poet William Talcott died in September 2006, his daughter couldn't notify most of his contacts because he kept their addresses in a password protected online account [**5 - 11**] and his Internet Provider refused to release the information due to privacy laws. The year before, that same provider had already had to be forced by a court order to provide access to the e-mail of a U.S. Marine killed in Iraq to his father [**5 - 12**]: the issue, however, is still open, also because it isn't clear yet if it's a privacy or property rights issue. In the meantime, the only thing to do is to make very clear (on paper, please!) who you want to have access to your computers when you die!

This isn't even just a family problem: it can seriously impact on other people's work and financial security. In 2002 a Norwegian researcher took to the grave the password he had chosen for an electronic library index [**5 - 13**] which would have taken about four years of work to recreate.

Probably the only safe solution that remains is to write down all these data on a sheet of paper put alongside your will or in a safe with other important papers anyway. A more technically savy solution would be to write everything in a file, encrypt it, write the corresponding password in a letter stored in your safe deposit box and distribute the encrypted file to some trusted individuals.

It is equally essential to remember the opposite side of the coin: what if some fatal accident happens to you while your computer still contain files, from old pictures or love letters to logs of chat sessions, that you wouldn't like others to see?

Malicious software

Some malicious software programs, whenever a computer is connected to the Internet, can report to a remote website the user name and Internet address of the computer, which programs were installed on it and which sites or files had been visited or downloaded from the net, all this obviously without giving any visible sign of activity. Such programs could also destroy important documents stored in the computer, or secretly transmit them to third parties. Technically speaking, no private or public computer owner can guarantee that nobody is playing such tricks on his or her computer, unless they have complete control on both the software [**37**] and the hardware which are used. The users who are not computer experts, instead, should still be able to install software which independent professionals have had the possibility to check and certify as free from such dangers.

Conclusion

All these are examples that a digital world makes it much easier to violate our privacy, but not in the way we believe, and that it is not "the Internet's fault". It is true that today it is much easier than ten years ago to spread false rumors or private information, or even bully teachers or school mates online. At the same time, even if these problems do exist and cannot be ignored, there are many interesting online services that would be impossible or much more difficult to use without computers and the Internet: what is important is that, even if you can't understand the technicalities, you are aware of the things that may be happening under the hood, and let them happen only if, when, and how you want. As this book will show, it's not so difficult.

Chapter 6

What are Biometrics and RFID

You are a password. Always the same

Originally, biometrics was that branch of science which performed statistical analysis of biological characteristics. Later on, the word started to indicate any technique for identifying people, with a computer, against unique physical characteristics like fingerprints, voice or retina. Sounds cool, uh? Almost too good to be true. In fact, it is too good to be true, unless it's very well thought out and designed, something that could be still impossible to achieve.

Behind all the fancy equipment and the cool living-in-sci-fi feeling, all the biometrics circus is still just about passwords. What happens when you type a password? The computer translates it into a sequence of bits and if that sequence is equal to the one already in the system, you are in. What really happens, instead, when a computer captures your retina or fingerprint scans, DNA sequences or anything else of that kind? The final result is nothing more than a digital description of that part of your body that is, again, just a **reaally** long sequence of bits: a password, nothing else. This second sequence of bits is simply supposed to be much better as an identifier than a traditional, typed one because it is:

- unique to you (and cannot be transferred to anybody else)
- so long that is impossible to guess it by pure chance and...
- unlike typed passwords, it is not necessary that you remember, learn or ever see it at any time

This is the real difference, the real advantage: with biometrics, **you** become the password. This is also the really critical *disadvantage*: unlike passwords, you cannot be reissued. What if a cracker [**12**] intercepts and duplicates that bit sequence corresponding to your retina or fingerprints? Traditional passwords can be changed; if you lose your ATM or credit card you can have a new one with a different code. Can you, however, replace your perfectly working retina or finger with new ones? Should you do it, just because some company didn't secure its computers? Who is going to pay for surgery?

The reason to bother about this stuff is that we're already past the phase when it only happens in science-fiction or top-secret military facilities. It's already in our normal lives because it already is a billion dollar market.

Shopping with your fingers

In June 2006 a convenience store in Tampa, Florida, announced that it had installed a device that scans fingerprints to process payments through a debit account [**6 - 1**] without cards or PIN numbers to remember.

Many other small and big companies want to do similar things because it is another, very promising way to reduce jobs, er.. costs. Payments made in this way would be faster and possible without the usual fees even on debit account or electronic checks payments.

The Tampa shop obviously pledged to keep all this personal information strictly private, but biometrics data are much more dangerous to leak than credit card numbers or ATM codes. Anybody willing to use such systems should give much bigger guarantees (that is, spend much more money on computer security) than they did in the past.

Another weakness in the arguments for recording customers' fingerprints is that privacy wouldn't be a concern because the fingerprint images are not the same as those collected by central Governments or law enforcement agencies. This is true, but even the fingerprint images collected on an actual crime scene are never exactly the same as those stored in police databases. In spite of this difference, they're still able to match them, just like you can recognize the same person in two different pictures.

How to duplicate fingerprints at home

Wherever huge quantities of money change hand there will be somebody working hard to steal some of that money. We already know about false ATMs and credit cards. Unless biometrics systems are very carefully planned and deployed, false fingerprints could make frauds much easier through biometrics, and it is **already** possible to make them.

In 2006 a Japanese mathematician and amateur scientist succeeded in fooling fingerprint recognition devices [**6 - 2**] with replicas of human fingers that he had built with dime store modeling compounds or dentist materials. The result was good enough to trigger virtually all of the most sophisticated biometric devices. The same guy also showed how to capture fingerprints from drinking glasses and similar surfaces.

Replaceable biometrics?

How can we protect ourselves? What if, five or ten years from now, all the stores in our area replace cash, ATM and credit card payments with biometrics? At the very least, they should assure us that their system is as at least as re-settable as the one they replace, that is that when (not *if*, **when**) somebody copies the bits they can be voided and replaced. If it's really going to be biometrics some day, it had better be replaceable.

IBM, for example, is already working on this. In 2005, they announced that they are developing some software that can transform biometric data like fingerprints into distorted models that still preserve enough actual identification markers [**6 - 3**]. These models are still usable but irreversible: it is impossible to recreate the original digitalized [**1**] fingerprint by looking at them.

If a store, bank or other organization only keeps a copy of the distorted model, it's not a big deal anymore if somebody cracks the computer where it is stored. Even in such a case, no *criminal* would have your real fingerprint, and another model can be regenerated.

In such a scenario, fraudulent access to biometrics data would become much more similar to stolen or lost credit cards: bad, but not irreparable. As long, that is, as you don't need to call the bank with a fingerprint protected cell phone, or drive there in a car that will only start with your retina.

The risks of RFID

RFID means Radio Frequency IDentification. It is a technology that makes it possible to build and use special integrated circuits (tags) which can be detected and read via radio waves when they pass close enough to an antenna of the right kind. The tags are very small (like a grain of rice) and need no batteries or other power source to work [**6 - 4**]. The radio signal generated by the *antenna* induces in the tags an electric current which is powerful enough for the tag to send a response.

RFID technology is making possible a huge range of practical applications and useful services. When you lift the last carton of milk from the supermarket shelf, an RFID tag on its bottom can immediately inform the shop manager that it's time to refill that shelf. Anything, from pets to guitars and whole containers can be tracked in this way for inventory purposes or to prevent theft. Giving up RFID would not make sense but, as any other technology, it should be used and regulated with much more awareness than it is currently happening.

One problem is that the cheapest and most common RFID tags don't know that they have left the store: until they break, they will merrily answer to all queries in the same way, sending all their data, no questions asked, without alerts. Once everything is sold with an RFID tag, walking by an hidden RFID reader will tell its owner who you are (as explained in the next paragraph), what you are carrying around and, with the right database connections, when and where you bought it. A solution for this could be to use tags that can be turned off when an item is purchased, but there is another category of issues to face.

How many passports of yours exist?

Several countries are issuing RFID-enabled passports, or plan to do so. The reason is obvious: an RFID tag can contain way more data than could ever be written on a few sheets of paper, and an airport employee would be able to read and store them all on his or her computer without even asking you to take the passport out of your pocket. The problem, as a BBC reporter found out in December 2006, is that the current RFID passports tags can be read and perfectly cloned in less than five minutes [**6 - 5**]. All it's needed is the right software and two hundred Euros worth of equipment that can be easily purchased online.

No RFID? No job (or assistance), thank you

In 2004 a study was conducted to evaluate the possibility of implanting tags in the arms of US hospital patients [**6 - 6**] to better track them. Other companies suggested that millions of Americans be implanted with an RFID tag for medical purposes [**6 - 7**]. In 2006 a Cincinnati video surveillance company required its employees to carry human implantable tags [**6 - 8**] to be identified. All these are only some of the reasons why RFID have been defined "Big Brother in small packages" [**6 - 9**].

Is technology enough?

Of course not. Choosing the right biometrics or RFID technology and waiting until it's mature enough is only half of the solution. It is equally essential that all the central organizations which would manage the biometric keys databases and the procedures which regulates access to those data and related analysis. These, however, are political problems to be solved politically, just like in any other case when personal data, encrypted or not, are involved [**4**].

Chapter 7

Should all the computers and computer programs of the world be equal?

What would life be like if there were only one type of computer and only one software program for every task? Apparently, it would be wonderful, right? Learn the bare minimum once, use it always. Just like pen and paper.

Reality is pretty different, however. As the environmentalists like to remind us, diversity is important. Its lack can greatly impoverish humanity as a whole. As M. Crichton puts it in "The Lost World", in a world completely dominated by the mass media and a completely homogeneous digital culture there would be *"less of everything except the top ten books, records, movies, ideas"*. Diversity is life, and wealth, and serious business for everybody. If it happens in the right way, this is true even with digital technologies.

Does your computer have the Flu?

AIDS or the bird flu scare us all a lot because we are all aware that, as far as immunity from diseases is concerned, we really are almost equal to each other: if only one sample of a virus figures out how to kill the human being unlucky enough to walk by in that particular moment, billions of other people will be in trouble in a few weeks time because, being very similar, they're probably just as vulnerable as the first one.

If this scares us, we should be similarly scared to have all the computers running our businesses or defense systems, or those running the pension, health and banking databases, running the same software: it might only take one virus to bring them all down, and once it happens... goodbye insurances, tax records, bank and credit card transactions. As a matter of fact, we waste many millions of dollars every year to prevent just that.

The protection coming from diversity just "happens", with humans, since we are (still) free to mix our genes more or less as we please, that is, from this point of view, to continuously develop new "variants", many of which will be immune to any given disease.

For the same reasons, that is the survival of an advanced human society, we should all encourage diversity and continuous interbreeding among software programs, even if it looks like much less fun. Especially because there already is somebody who is doing all the hard work for us, that is writing as many kinds of software as they can conceive of, and making a huge deal of leaving everybody free to do the same and share that software [**38**].

This is extremely important also because the right to free speech is already guaranteed, at least in principle, by many governments: in practice, however, today it cannot happen without the maximum availability of software.

Iceland, for example, is a sovereign State with culture, language and traditions which are at least one thousand years old. Back in 1998, however, Icelanders were told that sure, they *could* use computers just like everybody else, just not in their own language. Why? Because the maker of the most popular word processor and operating system didn't feel prepared to translate them into the Icelandic language [**7 - 1**]: too small a market, sorry, please **only** use English. Today many native populations in Africa, Asia and Latin America are still struggling to get out of the same trap. They cannot improve the quality of their life and be truly independent without introducing computers in their workplaces and Universities. But they cannot preserve their heritage and language, that is they cannot be really free, if they cannot use those same computers to write and work in their native language.

Luckily, the solutions to this problem already exist and are being successfully implemented in many developing countries: they are the same software applications mentioned above. All the "first world" nations should do is to follow the example of those countries, that is refuse outdated technology, and above all make sure that there are many alternatives, that such alternatives continue to be both legally and practically usable and that they are completely compatible with each other. We'll see how this can happen in the rest of the book.

Chapter 8

Do We Still Need Papyrus?

Yes. As a matter of fact, we all still need something similar to the ancient Egyptian superpaper that is still readable 4000 years later. One of the reasons remains the same for which all of our culture is in danger, that is, the disastrous mess which software misuse is leaving us in: nothing less than forgetting, faster every year, what we are doing and why, even when there are human lives at stake.

The nuclear-powered aircraft carrier Nimitz [**8 - 1**] was launched in 1972. The files containing its mechanical diagrams, whose availability is critical to ensuring proper maintenance of the ship, are already incompatible with modern software [**8 - 2**]. On July 20th, 1976, the Viking Lander became the first spacecraft to operate on the surface of Mars, collecting a lot of extremely valuable information. Only that twenty-seven years later, it was necessary to track down printed copies of those data and hire students to retype everything [**8 - 3**], because nobody understood anymore the format of those documents [**40**].

In 2005 the UK Atomic Energy Authority (UKAEA) started an 8 billion pound project to dismantle 26 atomic reactors. The plan is simple: collect all the radioactive waste, bury it in concrete bunkers and make sure that everybody living in their vicinities *for the next five thousands years* knows that they must avoid those bunkers and why. Five millennia is a long time: somebody said that if you really want any instruction you have given to others to be followed for so long you must start a religion about it.

While UKAEA did not start a Nuclear Waste Awareness cult, it was forced to exclude the usage of computer files, because so far their average duration has been even less than the two decades of the Viking data. UKAEA had to go for something a bit more reliable: a modern version of papyrus [**8 - 4**], that is a special kind of paper which, just like papyrus, won't discolor or rot. Three sets of the documents have been prepared, and will be stored separately.

Making good, old fashioned hard copies of important information is always a good idea, but we are all wasting a lot of money and time **today** because the preservation of digital information is anything but reliable.

One might not care less about what might happen to the Britons of the 25th century, or one might hope that the Nimitz will be many thousands of miles away the day when its engineers won't be able to figure out from the diagrams how to fix a broken engine.

Even in that case, however, government agencies must be accountable, today and over the next decades, to citizens, government officials, courts and auditors. In order to do this, they are already spending a lot of public money because yes, we do live in a digital world, but it is such a broken one that the national archives of many states [**8 - 5**] are not **allowed** to preserve documents only in digital format. Unless this mess is fixed, we'll indeed still need papyrus, but only have that. Until that day we'll have to give up not just the money that must still be spent on paper and storage space, but also the reading of public documents online, at no cost, from everybody's home or School.

Chapter 9

What do I really lose without Net Neutrality?

How Would You Like Your Network, Sir? Smart Or Stupid?

Net Neutrality is a somewhat misleading definition for the principles that, until today, have de facto ruled Internet based communications: access to the network should be open, at the same conditions, for every legally operating publisher or service provider. In other words, network operators should never block or slow down access to a website depending on the content of that website or who its owners are: the network should also be *stupid*, that is unable to distinguish the bits of a movie from those of an email, and move them around all at the same speed, leaving any decision on what to do with them to the user terminals.

This is not philosophy, completely detached from our world: once again, it impacts on our wallet directly, and our freedom. A world only made of smart networks is concretely and deeply different from one made only of stupid networks.

Smart Networks are those in which every channel is strictly monitored and regulated by very complex central equipment and policies. They are capable of services which are still impossible in other ways, because they are reliable. You get what you pay for. Inside a smart network you can call 911 and they **will** find you, because a Smart Network **knows** without uncertainties where you are calling from [**32**]. If anybody tried to leave 1000 Viagra offers every day on your answering machine, he or she would go bankrupt, or to prison, very quickly.

A Smart Network guarantees that you can call a doctor, or the hospital, even if all the teenagers in your neighborhood are downloading huge Playmates calendars just at that moment, or if the Superbowl is being broadcast, on the same wires, to the whole Internet. Because a Smart Network can tell the Superbowl or Playmate bits apart from the ones carrying your voice and force them to follow separate paths, without disturbing each other. And it always knows in advance which services are present and what their characteristics are, because only authorized, known services can live inside a Smart Network.

At the opposite end, in a Stupid Network anything goes. Even if complete anonymity is an utopia [**5**], you can easily achieve, or at least *feel* enough of it to be comfortable enough in most cases. If you invent a cheap, efficient software for online publishing, you can share or sell it online and million of other people will immediately be able to finally practice their freedom of speech for real: without permits to obtain, extremely complicated compliance tests, nothing. On a related note, have you ever realized that you can create and own how many email addresses you like, all different, for none or very little money, while the same thing is just impossible to do with phone numbers?

Please compare the cost, effort and legal hassles of starting a broadcast TV station with those, infinitely lower, of starting a web service like YouTube [**9 - 1**]. Or the costs and efforts of getting space on commercial TV channels with broadcasting for free to the whole world your belief that your company is putting lives in danger, as an engineer did in August 2006 [**9 - 2**].

All these are examples of the power of Stupid Networks. But the current Stupid Networks cannot guarantee that email will arrive instantly, or that your Bank website will always be reachable, or usable at the optimal speed, when you need to pay a bill. In a

Stupid Network 911 may be unable to rescue you [**32**].

Only in a Smart Network you are sure you will get what you pay for. But the menu will be much smaller and above all, only very few chefs get to write it and fix the prices. This point of view is elaborated online in the Net Neutrality Frequently Answered Questions [**9 - 3**]. In a Smart Network service providers and consumers are very clearly defined and kept separate.

We already have working examples of both situation. Fixed and Cellular phone networks, as well as Cable Tv are Smart. The current Internet is Stupid. The reason why "Net Neutrality" is a very hot topic these days is convergence: modifying the current Internet in such a way that any conceivable service can be moved to it. Running only one network for everything would immensely reduce costs, with theoretically great advantage for end users, not just stock holders: this, however, is only possible if the network is strictly regulated, er, Smart. This is why there is such a strong pressure to end Net Neutrality. Of course, the desire to prevent new service providers from entering the market also plays a significant role.

It is important, however, to make sure that if all networks have indeed to be merged and regulated in only one way, this doesn't prevent new services and voices from appearing.

Please ask your Parliament Representative what he or she is doing about this issue. In December 2006, a bill against Net Neutrality was rejected by the U.S. Congress [**9 - 4**]. In March 2007 some Democratic members of the U.S. House of Representatives called on the U.S. Federal Communications Commission to take a stronger stand for net neutrality (which is) an "indispensable policy for the future of the Internet" [**9 - 5**]. The general issue, however, is still open.

Chapter 10

Are computers really needed in (basic) education?

Information and Communication Technology is an essential part of any complete, modern education. Computers are already replacing pen and paper as basic, necessary tools to find a job or accomplish several everyday tasks. This started about thirty years ago: less than two generations ago, which is extremely fast on a global scale.

It is for this reason that, in spite of the media hype about how empowered and productive we all are thanks to computers, most of us still look at them with a sense of fear and inadequacy and know almost nothing about how they work. The result is that everybody proposing to "teach kids about computers" is greeted with gratitude and an open wallet, and anything done with computers looks cooler and self-justifies itself.

Too much technology, however, doesn't guarantee good results. A study on the effectiveness of education technology released in April 2007 by the U.S.A. National Center for Education Evaluation and Regional Assistance found achievement scores "were no higher in classrooms using reading and math software products than in classrooms without the new products" [**10 - 1**].

Too much technology can also seriously dumb down young people [**10 - 2**], if it isn't proposed in the right way, at the right moment and in the right order. It may be useless, for example, to learn computer programming at any level before integrating computers in the existing curriculum [**10 - 3**]. Consequently, there are four simple things to check before saying "Yes, let my children use computers".

How early is too early to start using computers?

It is very likely that computers as study tools don't provide any meaningful advantage to children who haven't really yet mastered what are popularly called the "Three R's", that is Reading, wRiting and aRithmetic. If this isn't guaranteed, sooner or later the results show, and they aren't pleasant. The author has personally known several Senior High School students who could not mentally multiply by powers of ten without a pocket calculator. A recent study in Italy found that many *University* students "could not articulate thoughts" [**10 - 4**]. "They write theses as if they were cell phone short text messages", the Rector said. The average level at some Universities was so low that they had to organize introductory classes to re-teach punctuation, grammar and so on.

Even in the absence of such excesses, most parents will agree that time passed in front of almost *any* screen, especially alone, should be minimized. Not because computers are evil, but just to enjoy life more and to learn first things first.

Are there clear goals and restriction on computer usage?

At least until 10/11 years of age, computers can find a place in study and school activity only if the children receive them to do something *specific*, rather than being just abandoned in front of a keyboard. Otherwise the computer would become simply an excuse not to teach, or at least a source of distraction and a waste of time already denounced by several parents in the Wall Street Journal [**10 - 5**]: specifically, every computer provided for study with public money to children in that age range should have really strict content filters [**29**].

Do teachers force students to think and look for substance even when using a computer?

Children who are told to use a computer for study "just because", often only learn how to waste time and be superficial. One of the mothers mentioned in the Wall Street Journal article found out that the laptop encouraged her son to behave just like many grown-up managers with masters degrees from the coolest Universities: he would spend more time finding the fanciest fonts than "digging through library books". In addition to this, all a child can learn by doing research online without strict supervision is how easy it is to copy, paste and **believe** whatever is found in the first two minutes spent with a search engine or online encyclopedia [**10 - 6**]. This is perhaps the greatest danger of all: to end up, in just a few more years, with *teachers* "formed" in this way, hence unable to conceive of anything better.

Are the teachers really motivated and up to the task?

Too many teachers, especially in primary school, are not prepared yet to use and propose computers effectively, or don't even believe it's really useful to do so: often this isn't even their fault. Many of these people are very responsible, dedicated and well-prepared in everything related to traditional teaching. Often, however, they barely know how to operate a mouse [**10 - 7**] and have no interest at all in ICT [**10 - 8**]: they are "teaching" how to use computers, often with little or no decent training for themselves, only because some central Government Regulation said so. In such cases, the only solution is to discuss the problem openly, encourage them to ask for better assistance and training and support their requests towards the School Administration.

Don't be afraid to ask!

Don't accept computers in the classroom or for homework unless you have personally checked with the teachers that they **want** to avoid these dangers and know how to do it. The next and last thing to do is to verify if the curriculum is designed properly [**47**], as explained in the corresponding chapter.

A word on the ultimate "Children Machine"

The "Children Machine" is the current name of what was initially named "The 100 Dollar Laptop" or "One Laptop Per Child" Project [**10 - 9**]. This mini-portable computer is to be purchased in very large quantities by the nations of the emerging world, which would then give one laptop to each one of their children. The reason to do so would be the chance to *"leapfrog decades of development - immediately transforming the content and quality of their children's learning"*.

During summer of 2006 some countries like Nigeria had already ordered a lot of units, while other important markets like India officially said "no, thanks" [**10 - 10**]. The reasons range from lack of trust in the project founders [**10 - 11**] to the same general doubts expressed in this chapter, that is the fact that children, especially poor ones, need a lot of other things before *any* computer.

While only time will tell if the Project will succeed as its founders expect, the Children Machine remains a good thing because it may have very positive impact on computing in general, if not on education in developing countries. Even if nothing else should come from it, this Machine should teach a lot, both to designers and to the general public, on how to give to the great majority of people all and only what they really need from computers: reading, writing and arithmetic at the smallest possible cost, without wasting electricity [**20**].

The interest around the project may also spark an interesting debate: if a 140 US dollars object is enough to *"leapfrog decades of development - immediately transforming the content and quality of their children's learning"*... why isn't it offered everywhere? Why should families in other countries have to spend much more, directly or indirectly, to achieve the same result?

Chapter 11

Is it OK for a School or Charity to accept software donations?

Families and students are just like public schools, churches, non-government organizations and charities of any kind: they all are on a shoestring budget but, sooner or later, cannot avoid using computers.

When this happens, sometimes one or more private company steps in, maybe through government programs, and offers computers or software packages. Money-wise, these all look like very good deals, maybe the only way some students or a charity could afford a computer. In some schools, the same offers may also be the only way to work on the projects the teachers assign to their students. Can parents and volunteers figure out if these really are good deals, without any hidden traps? Sure. As with everything else in this Guide to Family Freedom, no technical expertise is necessary: all you need is good old fashioned common sense and, of course, a list of the right questions to ask.

Are the pupils or members of the organizations prepared to use computers? Do they need them?

Don't let the board or anybody else spend your money unless they have demonstrated that there **is** something strictly connected to the organization's mission that will actually be done with the computers; or, in a school, that the teachers **are** prepared to teach their usage and that the computers are configured to avoid distractions.

Do these offers create dependence?

Yes, dependence, the same as with Drugs, or Alcohol, or Smoking. The dependence you find yourself in when you realize something has become dangerous, or at least useless and ineffective for you, but for some reason you are forced to keep using it. In case you were wondering, no, this is not (necessarily) an attack on computer games. We refer to the already mentioned fact that software has some dangerous characteristics that, like radioactivity from nuclear power plants, can create problems even after you have stopped using a particular program [**3**].

Do these offers force other people to waste money?

High School and University students can, in many countries, purchase some popular software programs at heavily discounted prices, for personal usage on their own computer. Offers like these look particularly tempting especially when a family **already** owns a computer. Before opening your wallet, however, please check if your computer is, or can become with little extra money, powerful enough to run that program. Don't trust advertising, ask relatives and friends who have the same or similar computers. Otherwise one may end up buying and might be forced to buy a whole new computer [**19**]. Any software that forces you to buy a new computer has a cost pretty bigger than zero. Note that this is true even if you had done something so stupid and unnecessary as illegally copying, rather than purchasing, that software [**36**].

Another thing to remember is that yes, we may be in the Third

Millennium, but in almost all jobs and fields of study, all a computer really needs to be is an integrated typewriter, calculator, email program and reader of Internet pages. Today, even some cell phones have enough computing power to do this stuff. Don't believe that you can't live without software so powerful that it only runs on the last generation of personal computers. Especially because there already are alternatives which are more than adequate for most small and home office users [**38**].

Chapter 12

My child wants to be a hacker. Should I worry?

Just yesterday, Junior announced proudly "I want to be a hacker when I grow up". Should I send him to a counselor?

Not at all. As a matter of fact, you should *encourage* your children to become hackers. Regardless of what mainstream media keep saying, being a "hacker" is not a bad thing.

It is true that mainstream media routinely use the term "hacker" to describe software-based criminals, those who break into somebody else's computer to steal private data or simply damage any file or service they can reach. No matter how common this usage is, it is still wrong: it seems created just to strengthen the perception that only people with some official authorization or assignment can study or modify software.

The correct definition for a software-based criminal who damages computer systems or steals their data has always been "cracker". A hacker, instead, is somebody who knows how to look under the hood of a computer and likes to do it, but only to make the hardware or software **[3]** run faster, or do something that, even if it's just one extra software function, was impossible before.

This is not a secret. Actually, it's one of the oldest computer slang terms around, widely accepted and clearly documented for more than twenty years [**12 - 1**]. Finding software-based criminals labeled as hackers in a magazine is one of the easiest proofs you can find that its articles (at least those covering Information and Communication technology or ICT) are written without any serious knowledge of the matter. You'd better complain with the editor, or simply shop for a more professional magazine.

The basic traits of a hacker, besides being a good guy, are activity and the desire to learn how things work, to improve them or create better ones. Nothing to do with playing videogames for hours, or doing something so uselessly stupid as illegally downloading music, movies or software [**12 - 2**]. Being a hacker is a cool pastime for a teenager, and it may very well turn up to be one of his or her wiser career-preparation moves.

Hacking is not limited to software. A good example of hacking everything, and a great resource too, is the Make Magazine [**12 - 3**], which has been defined by the San Francisco Chronicle as *"the kind of magazine that would impress MacGyver"*. Make Magazine proposes and explains projects on anything from high speed photography to backyard biology, and everybody can contribute!

Hacking is good and is an excellent exercise for the brain: it's what enables young people to turn an original dream into a successful and really rewarding job. What hacking is all about is finding solutions that legally and pacifically improve or change the state of things. Maybe this is the reason why the confusion between hackers and criminals is encouraged or tolerated in mainstream media. All children should be hackers. Let's make sure that misguided laws don't prevent this from happening.

Chapter 13

My children ”share files” with their friends: are they always criminals?

The short answer is ”yes, if they have no explicit permission to do so from the author of those files”, regardless of what those files are: songs, movies, games, texts or software programs. If you forget this, you may hurt both yourself and others.

You Got Lawsuit

In May 2005, D. Bink of Milwaukee was sued by the recording industry [**13 - 1**] for the downloading of hundreds of songs. The choice he had was to immediately pay 3,750 US dollars to settle or go to court, *”where he may be ordered to pay at least 750 dollars per song”*. Mr. Bink can barely turn on the computer but, two years before the lawsuit, his teenage daughter had downloaded for free several songs from the Internet. He was the one to be sued because the family Internet connection was registered in his name. Mr. Bink decided to fight the lawsuit in court, even though it could cost him more than 10 times the settlement offered, but how many families could, if trapped in the same situation, afford such a luxury?

This is not a hypothetical question. Since 2003, the recording industry has done the same to more than 10,000 families. Their justification is that every album which is not purchased, but downloaded gratis from the Internet is a net loss for them. Therefore, they say, *"it is critical for us to send a strong message to individual users that you can be caught and there are consequences for your actions"*, counting on the fact that *"the United States Supreme Court ruled unanimously that the uploading and downloading of songs, in violation of copyright, is illegal* ***[13 - 2]****"*.

Since almost nobody knows how to write by him or herself a software program to find or share files online, the recording industry also goes after the people who write and distribute such programs. This software, however, is also used to share a huge amount of legally re-distributable computer programs, or multimedia content. Since such legitimate uses exist, you have no justification if you use those programs to perform illegal downloads: the fine print on every file sharing program or website invariably says that it is only (and rightly) **your** responsibility if you use their software and infrastructure to violate copyright laws.

The industry, in any case, couldn't care less: if some software *could* hit *their* wallet in any way, its developer, even if he or she is a teenage student, cannot be allowed to develop it.

In year 2000 a Norwegian teenager was arrested for having broken, with almost no effort, the DVD encryption scheme. You might have heard this referred to as the DeCSS trial. This boy has been prosecuted by the movie industry with all their powers, and treated (by some press at least) as one of the worst criminals of the decade. And then he was cleared of all charges only three years later. The program written by that Norwegian hacker, and the way it's supposed to be used, however, are perfectly legitimate. What that program makes possible is to play a regularly bought DVD on your computer even if the DVD software of *your* choice is not on the officially supported list.

Is there a limit to this madness? Is it madness?

Some people see all this as a necessary evil by way of transition to a new, copyright-free age [**13 - 3**]. They argue that, if the record companies sue their fans, alienating their audience and victimizing people who don't even realize that what they're doing is wrong, eventually those companies will go bankrupt and collapse.

Unfortunately this strategy is either too risky or very inefficient. So far, all it has produced are good pretexts to mess up people's lives; in the long run, it may just give good excuses to reforms of technology that give no more choice or escape routes to end users. Think about it: all the law proposals for worldwide enforcement of DRM [**16**] or Trusted Computing [**17**] schemes which benefit only some multinationals are justified **exactly** with reports of millions of illegal music and movie downloads which actually take place every month. If both this activity **and** the legal purchase of those same songs and movies stopped, even for just a few months, those lobbies would have nothing at all left to justify their requests and would quickly have to find other business models. Remember that corporations are just as powerful as they are fragile: even two consecutive quarters with no or lower profits could lead any company which lives on the price and reputation of its stock very close to bankrupt.

Back to tolerating or advocating illegal copying: don't forget that, besides end users, laws and technologies like the ones just mentioned would also hurt or lock out from the market many independent artists (including, in the future, your own son or nephew...) who don't **want** to be submitted to big corporations.

What can we share then? Are there any legal solutions?

Sure: one way to go is to only share material which is surely in the public domain or your *own creative works*, according to the current definition of "yours" [**15**]: fully original stuff that **you** have created. The real solution, described at the end of this book, is to act for a reform of some laws that puts an end to these excesses. Until that happens, however, and also to accelerate it, it is much smarter to **bypass** and leave without arguments, as specified above, all the companies which damage both actual artists and their fans.

Should I really give up music, movies and so on?

Not at all, you just have to be smarter and not jump on what looks like the cooler and trendier bandwagon. It all depends on the license, that is, the legal limits the author of the creative work has put on its redistribution (within the limits of copyright law, of course!). Luckily there are already a lot of artists, as well as programmers, in many fields, who do not have to feed greedy intermediaries or can and want to share, in a more liberal way, the result of their work. Many of those artists explicitly allow you to legally share and reuse for free their songs, text, movies or pictures, and their works can be easily found online thanks to special purpose search engines [**13 - 4**].

Remember: if you don't support with your time and wallet only the authors who try to reach their audience with as few intermediaries as possible, the consequences may be pretty serious, and some of them would also be your fault.

Chapter 14

I Can Record TV Programs, Can't I?

This may certainly seem as a stupid and unnecessary question but unfortunately, depending on where one lives and what will happen in the coming years, this assumption may be far from true.

Before looking at the answer, however, let's define what time and format shifting are. The first term is what happens when you use technology to enjoy some video or radio show at a different time to when it was originally broadcast. Taping your favorite sitcom to watch it when you're back from work is time shifting.

Format shifting, instead, is when you copy or move some creative work to a different physical support. The reasons for doing it range from having an extra copy in case the first one breaks to saving space or simply "playing" that material on a different device. Scanning printed texts and photographs or copying music from vinyl albums to a portable player are common examples of format shifting. Besides private use, format shifting can also be done by institutions. Public libraries, for example, may download documents of any kind from the Internet to provide either paper or CD-ROM copies to their clients who cannot afford a computer or a fast Internet connection. In the reverse direction, institutions may save a lot of storage space and money if they could move tons of paper documents to a digital format. Unfortunately, as we've seen in another chapter, we're still stuck with papyrus and other legacy technologies [**8**].

Now, time and format shifting may seem to be something which can only be good, to which nobody could possibly object, but this isn't the case.

At the end of 2006, for example, in New Zealand there still was no general exception yet to *format shifting of legitimately purchased recordings [14 - 1] from one medium to another to allow playing or viewing via other devices.* Possible exceptions are still under evaluation [**14 - 2**]. In the meantime, format shifting doesn't appear to be legal in New Zealand. Even if it were legal, making a personal, backup copy of the CDs you purchased may remain illegal because... it's not format shifting [**14 - 3**], if you go from one support to another of the same type. Format shifting of DVDs, for example, was still not permitted at the end of 2006.

In Australia, the transfer of music from CDs to portable media players became legal only in May 2006 [**14 - 4**]. Even recording television and radio programs to watch them, privately, at a more convenient time, was illegal before that law. The new law proposed in Australia, however, includes bright concepts like making illegal things like "to lend a video copy of a TV show you have made to your family or friends if you have already watched that copy", or watching it yourself more than once [**14 - 5**]. The explanations for the same proposal explicitly specify that you cannot make a backup copy of a CD in case the original is lost or damaged, because a format-shift copy is allowed only "in a different audio format to the original".

Things are going to get worse soon

The new generation of high definition DVDs, players and TVs is only going to make things worse, sometimes even for those who do try to make content providers happy by trying to play by their rules.

There is a whole new family of technologies whose purpose is to provide high definition movies and TV shows to all consumers who can afford them. The two standards of this family which will very soon become familiar in all households are HDMI (High Definition Multimedia Interface) and HDCP (High-bandwidth Digital Content Protection). Their purpose is to let people watch high definition movies and show **without** leaving them any possibility to make *personal* copies of such movies and shows at the same quality. HDCP, for example, is *"designed to prevent the interception of data...between an output component and a display"*.

The high definition output connector of an HDCP DVD player sends out the high definition images of a movie in a encrypted format. **Only** an HDCP-enabled monitor can properly decrypt and display them. If the legal owner of such a DVD player and of an HDCP-protected disc tried to make a backup copy or reuse some scenes or audio from it for a family movie by attaching a DVD recorder to those connectors, he or she would not get any usable output. Images and sound would only be available through other output connectors of the player, but *at a lower resolution*, that is... artificially degraded!

An even funnier (so to speak) part of the story is that all these specifications are so complicated that many manufacturers haven't got them right yet. In January 2007, for example, several owners of the Playstation 3 game console found that their consoles, high definition TVs and connecting cables weren't compatible with each other, causing "the sound to cut out and the screen to blink on and off" [**14 - 6**] when playing some games!

Who controls your television?

(**Note**: The rest of this paragraph is a summary of a March 2007 report from the Electronic Frontier Foundation which is available online [**14 - 7**]).

Today, there are no restrictions on use after lawful, authorized reception: people can choose any device with whatever recording features they like best. To fix this, an inter-industry organization is devising standards to ensure that TVs and other digital entertainment devices obey content providers' commands rather than consumers' desires.

The restrictions of this new systems, called Content Protection and Copy Management (CPCM), include marking broadcasts programs as "Copy Never", making them impossible to record and replay too frequently outside your home, or on different TVs inside your home.

The reasons to block this time or format shifting is to force you to buy that show again on DVD or through another delivery mechanism. Even if you *had* already paid for it. CPCM-restricted media will also be able to carry blacklists and revoke compatibility with particular devices that don't enforce Hollywood's restrictions sufficiently. Playing a CPCM DVD may STOP and make your legally purchased player useless.

Besides limiting honest consumers, CPCM will also choke off innovation and competition by limiting who can enter the device or broadcasting market. Film makers could choose to only license content to providers who implement these traps.

All this would be coupled with laws which will make it illegal to manufacture or use tools to circumvent the DRM without the copyright holders' authorization, even if the circumvention allows a user to exercise her legal rights, or the resulting devices are much cheaper, smaller, or dissipate much less electricity. Please note that none of these restrictions need to be revealed in advance.

Chapter 15

Can I publish My Own Movies?

All modern camcorders directly save movies in digital formats. Even old VHS tapes can be easily digitized at home with relatively cheap living-room DVD recorders or computers. All this makes it very easy to mix any combination of home made or commercial movies for pure and innocent fun. Theoretically, that is.

You have already learned in another chapter that, should the recording of your Christmas home dinner include your kids singing some copyrighted song or watching some Disney movie, you may have to ask permission and (if you're lucky) pay loads of money for it [**2**] to be sure you won't be sued.

All this is so ridiculous that the temptation to just laugh at it and forget the whole issue is, understandably, very strong. Before going on with your life, however, please consider the following things.

First of all, even if the probability that it could happen to **you** is (still) very remote, there are lots of very real and expensive lawsuits of this kind going on right now [**13**].

In the second place, if nothing happens soon, the *next* generation of home entertainment devices may very well be able to take this innocent fun away without any need for anybody to throw one single policeman or lawyer at the problem [**17**].

The most important problem, however, is that "home movie" and, in general, "home project" can be terribly generic terms.

Regardless of how people in the street personally consider it, until the law says so, very common practices like the ones described here and in the previous chapters *are* copyright violations and copyright violation **is** a crime: this is just a technical/legal definition, not a moral judgment. In this context, there is a very important reason why most people can keep committing this crime or, more exactly, wrongly believe that they can afford to let things be as they are today. The reason is that they are only considering their *own home movies*, that is things that, quite frankly, there is no real, serious reason to publish at all.

In spite of the recent popularity of sharing websites for personal video clips, almost all of the authors of "home made" video will never have any objective interest or (financial) *need* at all to ever publish their work. Consequently, the actual chances of being caught for an illegal, but never-released home movie could still be small enough to be acceptable. As far as the rest of humankind is concerned, not to mention your relatives and friends... they can probably survive without ever knowing from the Internet what you had for dinner last Christmas, or which songs your children sang at their last school show.

So, if this were all the story, it would be still ridiculous and unjust in principle, but there would be no real damage to you or society as a whole. The problem is that some masterpieces and civil campaigns, that is things that it is *necessary* to publish for the common good, start just like that, as "home projects". If legislation and technology make *those* things much more difficult to do without lots of money or lawyers, now that's a surely bad thing, isn't it?

For the record, this is just what is already happening, with even more harmful consequences for education, with documentaries. According to the New York Times [**15 - 1**], in 2005 two film-makers were filming a fourth-grader child and his mother when the mother's cellphone rang. That was a disaster: since the ringtone was "Gonna Fly Now," the theme from the first Rocky movie, the copyright owner (which is not the actual author of that music) asked the first-time producer for 10,000 US dollars to publish those six seconds of documentary without the fear of legal suits. Eventually, they settled for 2,500 dollars (for six seconds of music included in the shot by pure chance...), but the total clearance fees, for the same reason, of the whole documentary, amounted to about *one hundred and seventy thousands dollars*! Eventually, the "Mad Hot Ballroom" documentary saw the light only [**15 - 2**] *"by limiting music played in classrooms, haggling over clearance fees, and cutting out a scene."*

As an Internet user put it [**15 - 3**] *"Considering the (USA) constitutional mandate to promote the progress of the useful arts and sciences, it is tragically ironic that copyright law keeps many documentaries from getting produced and drains the life out of others."*

This is the real reason why everybody should be upset if "home movies" cannot contain anything which already exists, and why all parents should immediately start asking for a serious reform of the relevant laws. Education, preservation of our culture, the next documentary from some unknown, shoestring budget director that denounces some serious problem or civil rights violation: all this could never happen if, for every single scene of their movies, authors had to spent huge amounts of time and money just to get permissions which may never arrive anyway.

Which way did you do that movie?

Besides the copyright madness issue, that is regardless of *what* you put in a movie, you must know that you are also required to be ridiculously cautious when you use some of these latest digital entertainment *technologies.* If the thought of publishing your amateur masterpiece ever came to your mind, the freedom of actually and fully using all these wonders of digital technology may be restricted to those with deep enough pockets.

More exactly, if you aren't careful you may find out that you would have to pay royalties even to publish **your** original movies on **your** own website for profit. This is exactly what can happen if you chose for your movie files the MPEG4 format [**15 - 4**]. The only safe way to avoid this danger is to use other formats and technologies, already available, which are free of these legal time bombs.

Chapter 16

What is this DRM thing I keep hearing about?

Definition and examples

DRM is something that is already having a great impact on how you access and enjoy every form of information or entertainment which is distributed in digital format [**1**]. Officially, the acronym stands for "Digital Rights Management", even if many people believe it indicates "Dementedly Ruined Music" or "Disgustingly Restricted Movements, Mirth and Movies".

Practically speaking, DRM is the set of technologies too often used to abuse copyright, that is to prevent people (or at least to greatly limit their options), from copying, modifying and reusing any digital material, even when they regularly purchased it.

Perhaps the most common example of DRM is the "Region Code" on most retail DVD movies. DRM is why your DVD player or computer won't play a movie that you regularly purchased online or during a vacation abroad, even if it will **never** be sold in your home country. Absurd, isn't it? It is perfectly legal to purchase stuff abroad, not to mention that often it is cheaper and much easier, if you have a computer, than it used to be. For a caring parent it may also be an excellent way to have his or her children practice a foreign language or, in a family of immigrants, to keep alive the culture and memories of one's native country.

Here's another DRM absurdity. Affordable homes become smaller every few years, VHS tapes take much more space than DVDs and their quality degrades over time. Any parent whose kids play "Winnie the Pooh" [**2**] every other evening knows that. In spite of this, thanks to DRM, that is the copy protection measures on many recent VHS movies, it is not possible to copy them on DVDs to save a lot of space and make **your regularly purchased movies** last as long as **you** need them.

Strictly speaking, these and many other DRM measures could still be easily circumvented. The only problem is that, in order to do it, you must either have software or hardware knowledge, or wait until a programmer breaks the DRM scheme and shares the solution with you. The real problem, however, is that in both cases people are forced to commit a crime, that is to modify in illegal ways **their** hardware or software, to remain able to use **their** tapes and DVDs.

Why the industry wants it

The entertainment industry is pushing very hard to make DRM ubiquitous for one simple reason: to make more money. Sure, DRM is first of all an attempt to reduce the number of illegal copies: too many people get almost all their movies and music from illegal copies just because it's easy, without giving anything back to those who actually created those works. Others make a business of making thousands of copies of a CD or DVD to sell them at much cheaper prices. In both cases there is an obvious monetary loss for the creators.

The second and more important reason to enforce DRM is that it's the only way to make format shifting [**14**] impossible, in order to sell the same thing over and over and create many (artificially) different markets. DRM is the opposite to globalization, even if it is advocated by multinationals.

What is bad or useless in DRM

There is nothing wrong in copyright as a way to reward, for a limited time, the authors and performers of creative works while granting fair use [**18**]. DRM *could* be good, or at least harmless, if it just ported these things and nothing more to digital works. Most of its current applications, instead, do more harm than good.

First of all, DRM as it is today is just useless against industrial scale illegal copying. It has been said that ”DRM doesn't stop online piracy [**16 - 1**] any more than a speedbump in your driveway slows interstate traffic”. The reason is that all digits are the same [**1**]: there is no problem whatsoever to copy **all** the digits on a DVD (both those constituting the movie and the DRM ones that should ”protect” it) on a million blank DVDs and sell them at a very low price. The only real solution to this fact of life is to make computers as we know them today disappear: this attempt is already taking place and is discussed in the next chapter [**17**].

In the second place, DRM goes right against fair use. The books you bought ten years ago can be moved to a new bookcase, rebound or get a new cover. You must buy a new copy only if they are destroyed, not if you go on vacation or start wearing glasses. You can sell or lend them. You **can** buy them in the first place. These same rights must remain (both technically and legally) even with digital works.

It must therefore remain possible to *purchase* a copy of creative works: otherwise, a very tempting way to legally limit consumer rights would be to stop *selling* them (or the hardware needed to use them) and only offer *leasing* of books, music albums, computers, DVD players... In the second place, legally purchased songs, movies or books in digital format should remain usable with any electronic device you own and freely movable from one of them to another, without absurd procedures or fees to pay.

What we have today, instead, is that ”as consumers, we can't decide anymore on what we'll watch. We watch whatever gets released where we live, at whatever prices they decide” [**16 - 2**]. So much for globalization.

Another big problem of DRM, another trap to avoid, is that it can seriously hurt not only end users but also many artists, as explained in more detail in another chapter of this book [**33**].

Last but not least, at the cultural level, DRM prevents preservation of what *people* find important: under DRM, only what looks important to *corporations*, because it can be sold times and again, is surely preserved and remains legally available.

How can you recognize and fight DRM?

It is very tempting and (still) very easy to just ignore this issue altogether and keep breaking, while it's still possible, DRM related techniques and laws. Doing so, however, gives the corporate interests which are pushing DRM the best weapon they could dream of, that is arguments to impose electronics devices which are impossible to use as you want [**17**]: black, dumb boxes that your children could **never** use to learn a technical job, create **their** own music or movies or start a business without bending backwards to some corporation.

With just a bit of self discipline, the right way to fight DRM is very easy to practice; after all, we aren't talking of food or medicines here. Just ask, before buying CDs, DVDs or any other creative work in electronic format, these simple questions:

- Is this usable with any type of software, computer, cell phone, portable player...?
- Is it technically possible to do a perfect, non degraded backup copy without messing with the hardware in any way?
- Is it possible to move this song/movie/whatever to other discs or devices without any limits or loss of quality?

If the answer to any of the questions above is "no" or "I have no idea", think at least twice before buying: almost surely, you would get something that you will be forced to buy again in very few years, if you want to preserve it. Note that this remains true even if you buy at a lower price, or get for free, any illegally copied (”pirated”) material.

Chapter 17

What is Trusted Computing?

In a nutshell, yet another thing that could do you lots of good or seriously screw up your life.

Let's start from this question: apart from licensing [**36**] and prices, can you, or the school and Public Administrations running on your money, freely chose any software and hardware combination *you* want and, above all, do anything *you* want with them? In a few years from now, the answer to this question may become "Yes, as long as they are in a list decided by somebody **else**".

Welcome to the world of Trusted Computing

A Trusted Computing (TC) platform is a computer, DVD player or any other electronic device which is able to provide reliable information about which hardware and software components it is running. People, computers or any other device can request that information and, reading it, decide whether it's safe or admissible to interact with the TC device. The software officially provided with a TC system, for example, may refuse to run if it detects that other software without the TC label is installed.

The trick is that, so far, it has been given for granted that this ability must be under the explicit and exclusive control of the platform's *maker*, not the person who eventually purchases it. A TC-locked DVD player may refuse to give you some information even if you legally paid for it. Practically speaking, this means that that a TC player may tell you "I will not play this DVD that you *legally bought*. Not because I can't, but because the movie company doesn't like the software that you have installed on *your* computer".

Similarly, the website of your bank may refuse to let you in from any "platform" that they do not trust.

Internet Access Providers (IAP) may use the same technology to forbid you to connect to the Internet (or be legally forced to do so) unless you do it with a TC-compliant computer: in other words, unless you install all and only the software on your computer that **they** (or the government) want.

The basic idea behind TC isn't necessarily bad: would you keep using ATM machines if they were proved to be as unsecure as today's computers? If you must use a computer to pay some bill online or perform some other equally sensitive operation, maybe from somebody else's computer, you *should* be able to know for sure that all the involved computer are in a state that protects your privacy, money and reserved data. Current computers do lack this capability. Therefore, a really effective TC wouldn't be so bad if end users maintained the capacity to *themselves* declare which software is acceptable on their machines. In such a scenario, inexperienced users may still sign some service agreement with their IAP to lease or purchase TC machines, while others may self-certify their systems (under their responsibility, of course).

What matters is that everybody, not just big corporations, maintains the possibility of designing or using any kind of software he or she considers best for his or her (obviously legal) needs. This is also a matter of security. If it's necessary to move to Trusted Computing, it is also essential that it works on as many different and independent software and hardware combinations, because this minimizes the risk that one defect in one of them causes serious problems [**7**], for example, to all the customers of all the world's banks at the same time.

As far as trust goes, it should go both ways, shouldn't it? When Trusted computing is concerned, this means that you should be really, really picky about which government or private *authority* is allowed to decide what you can or cannot do at home with the stuff you buy.

The problem is that, with all the TC designs proposed so far, definition and detection of "safe environment" rests entirely with the *original* owners of the hardware, software or information you need to use. If those "owners" are partners of movie companies which don't want people to make a backup copy of their *regularly purchased* movies, so they can sell them more than one time, what is the end result? Nothing more than believing to have bought a (pretty expensive) computer which can also manage movies, but actually getting a mutilated VCR, even if it's a really cool-looking one.

Can TC devices be modified?

The first time they encounter TC or DRM **[16]**, many people erroneously believe that, since they were so smart in cracking their satellite receiver or installing a cracked copy of some software for DVD duplication, they can safely ignore it. This time it is really different, however.

TC-capable hardware is neither so common nor supported yet that it can guarantee that it will refuse to start if the whole system (both hardware and software) is not in a completely trusted state.

In a few years, however, TC devices will include some extra hardware components, which **will not be possible to modify, remove or reprogram with normal tools**. Those components are just the ones which will decide if, when it is turned on, the whole system is in what *others*, not its legitimate owner, have defined as a reliable state.

If those components are programmed before assembly in the factory, according to the wishes of big media companies or software makers, *they* will decide what you can do with "your" computer, home theater or DVD player. For the first time, it will be not only illegal, but also physically impossible to turn off or circumvent the scheme in any way: it won't be possible to disconnect or control the relevant signals, as some experts do at home today, without breaking the device. All the corresponding signal lines and connectors will be completely embedded inside the board or some sealed integrated circuits. In such a situation, even **if** people will still be able to find non-TC devices in the stores, they may be useless for all practical purposes, from burning DVDs to creating your own music playlists or simply running the software tools *you* like better. According to some analysts, new computers without TC locks may become quite a rarity [**17 - 1**], if not disappear from stores altogether, as soon as in 2010.

How can I recognize Trusted Computing, and what should I do about it?

It's easy. Before buying any software, computer, or other device able to create or use music, text, movies or any other type of creative work, ask:

- does it contain a TPM or any other Trusted Computing component?" (TPM stands for Trusted Platform Module, a class of TC devices)
- if yes, can I still install any software **I** want on it?

If the answer to the second question is "no" or "I have no idea", think at least twice before buying, and explain why to the clerk.

Chapter 18

When Is Fair Use Fair Enough?

Before digital technologies and the Internet, just a few years ago, in order to duplicate music and movies on tapes or vinyl albums on other tapes or vinyl, you had to physically exchange them in the first place. Above all, the quality of any copy would have been worse than the one it came from: in practice, from every original album sold, only ten or twelve usable copies could be made.

Now that music or, for that matter, almost any document or creative work can be coded as a sequence of digits, everybody can make millions of copies of it, all perfectly equal to the original.

This can lead to great cultural and economical progress, on a scale never imagined before, and to great benefits for artists and authors, but only if accompanied to different laws and, above all, a level of responsibility and basic knowledge in the general public much more diffused than it is today.

Otherwise, the consequences can be very dangerous both for the *current* media companies (which is not necessarily a bad thing) and, potentially, also for the artists and authors who do the real work or the real service [**12 - 2**].

Sure, today if one person buys one CD, everybody else could have a perfectly equivalent free copy in a few seconds, remotely. In spite of this, some fundamental concepts have not changed, and it is better to set them straight for the common good. Using music or any other creative work for free while it is still under copyright, against the wishes and livelihood of the **actual** authors is not fair. The same applies if somebody installs a commercial DVD SW player or any other software on his or her computer without paying whatever the author wants, as long as there is choice among many different software programs and it is possible to create free ones [**38**].

Moving for personal use music or other digital works legally obtained to any other media or device, as many times as one wants and without limits of time, is fair. Public redistribution of material which is still under copyright, without paying anything at all to the author, is not fair (unless, of course, this is just what the author wants, as it often happens). Making one thousand copies of a copyrighted DVD to sell or distribute them, for example, is certainly a crime, and must be prosecuted. *And it was never different.* It's not like we're losing any existing freedom. Since when copyright was introduced, it never was allowed to go beyond fair use and fair use never included public redistribution. Besides that, there is a lot of choice out there. If artist X starts to ask too much for his or her music, just go somewhere else.

Forcing people to pay many times for the *same* personal copy of the same piece of music is not fair. Forcing every author to lock him or herself into a corporation, or to change his or her line of work to survive isn't fair either.

File sharing and unrestricted redistribution have every right to exist (almost a duty, actually), as long as they are used to share for free what somebody created (created, not bought) and then freely decided to give away, or when the copyright is expired. The common "wisdom", these days, is that copying music, movies or software without permission is never wrong, because copyright is an unfair privilege granted to a few companies, is in itself unfair and has no reason to exist. This *may* be true if thinking only of those companies, but it would also hurt artists, authors and society as a whole, both because the actual creators worked hard and because a lot of creative works would not exist otherwise [**12 - 2**].

Most of the problems created by copyright today are actually created only by its exaggerated extension in time. A copyright extended for many decades to all conceivable "uses" of creative works is only wanted by big media corporations, just because it is *the only thing that makes really profitable to create and operate such big structures.* A much shorter duration of copyright would make all the excesses of today not worth the effort, while still giving incentive to create many more works than would ever be possible through public or private patronage.

The fact that the duration of copyright has been unfairly extended beyond reason cannot be a justification to be unfair with artists and authors. It just means that it is necessary to reduce that duration, so that the actual authors can still get tangible benefits from their work, but the investment to *control* all of them is not convenient anymore.

Illegal copying, above all, is one of the most useless (hence stupid) crimes ever, because there are valid alternatives. It may even be the most effective way to give even more power and control to big corporations, so they can have even more control over your life and an even bigger slice of your money.

Such excesses are also influenced by, and influence in turn, how software is managed and developed. But you can and must, in your own family, do as much as you can to stop this self damaging behavior.

Chapter 19

Does Software pollute?

Of course it does. The average USA citizen, for example, produces 4.6 lbs of solid waste per day [**19 - 1**], and an ever growing part of it is software. Sure, software is just instructions, the immaterial part of a computer and many other electronic devices. As such, it should not pollute, right? Instead, it does: a lot. Obviously this doesn't happen directly. We pollute a lot by trashing too much working electronic devices of any kind and buying unnecessary others, too often.

In January 2007 the UK Green Party officially declared Vista, the new operating system likely to be installed on many millions of new and used personal computers, a ”landfill nightmare” [**19 - 2**]. The reasons? The fact that this software may ”force expensive and environmentally damaging hardware upgrades”. More specifically the fear is that an enormous number of monitors and other perfectly working hardware ”will be junked by consumers and companies as Vista will refuse to play the new high-definition DVDs with current monitors and sound cards”.

Potential risks for the environment do not come just from the need to control and restrict entertainment [**16**] or to sell ever more software or computers every other year. The Children Machines described in another chapter [**10**] are made according to the latest, more environmentally friendly regulations. Those laptops, however, are meant to be sold and used in countries which have no adequate recycling centers and no money or infrastructures to collect used computers. This is already raising serious concerns about the environmental impact of the whole "One Laptop Per Child" project [**19 - 3**] in a few years from now, when those laptops will break or be dismissed from use.

The reason to be concerned about it is that electronic devices contain many toxic substances: so many that in 2004 even a report of the United Nations University of Tokio [**19 - 4**] recommended to extend the lives of computers for this very reason. The report pointed out that, in that year *"a 2-gram memory chip required 1.3 kilograms (1,300 grams) of fossil fuels and materials"*, while a whole computer and a big monitor required *"1.8 tons of water, fossil fuels and chemicals to make"*.

Generally speaking, making hardware or any other high-tech digital object can be a pretty dirty job. In April 2000 the San Francisco Bay Guardian reported that several hi-tech workers were suing their employers because of serious illnesses [**19 - 5**]. Higher rates of miscarriage, some types of cancer [**19 - 6**] and premature death have been observed among the workers of semiconductor and hard disks factories in several countries [**19 - 7**].

Today all this still happens, just in other countries. Electronics manufacturing workers in Mexico and many other countries have just started to discover that they face the same health and safety hazards experienced 20 years ago in Silicon Valley [**19 - 8**].

The problem is not limited to the manufacturing of electronic devices: it remains even when it's time to dump or recycle them. Electronic waste or E-waste is the most rapidly growing waste problem in the world. In 2005 nearly 2 million tons of electronic waste, including 133,000 PCs discarded each day, were produced in the U.S. alone [**19 - 9**].

This is true even if many computer makers have indeed started to use more environmentally friendly materials and procedures. All around the world there is still a huge quantity of older components which were produced committing what a 2002 report called the Seven Deadly Sins [**19 - 10**]: these include usage of lead (brain and blood damage), flame retardants (hormones imbalance), and PVC cabling which generate dioxins when burned. Even in this case, often the world' richest countries are still simply dropping the problem abroad. Still in the U.S., only 10 to 15 percent of electronics are currently recycled, but in 80 per cent of those cases up to 80 percent simply means "exported overseas". The situation in most other countries is the same or worse.

The true cost of software upgrades

Replacing even one single software program may mean to be forced to replace a whole, still perfectly working computer, that is to contribute to the problem described above. It starts innocently: a computer has 512 MB (Megabytes) of memory but the next version of program X requires at least 600 MB just to start up (in a computer, the "memory" is the set of circuits used for temporary storage of data and intermediate, real-time calculations. Permanent data storage happens in separate *hard disks* which can be internal or external to the computer). But there is no 88 Megabyte memory stick on the marketplace, the minimum size is 256 or 512 MB. Since they cost only a few dollars, OK, no big deal, let's buy 256, right? Yes, but only if the the motherboard of that computer **does** have a place where one can plug the memory sticks they sell today.

At this point, in order to use "the next version of program X" the owner has already given in to buying more memory than is actually needed, plus a new motherboard to host it. Even if the program itself was obtained, legally or illegally, at no cost. But the new motherboard is, very likely, not compatible with the processor, the heart of the computer, so it is necessary to buy one of them too, please. Will the power supply connector of the new motherboard be directly compatible, without any adapter, with the power supply socket on the motherboard? This is not a big deal, especially because it only matters *if* the old power supply is powerful enough to handle the current motherboards and processors.

Does it end here? Maybe not: the scanners, printers, external modems and tablets one could buy a few years ago have connectors which are not necessarily present on all the motherboards sold today. If this is the case, it's time to figure out what is less expensive and time consuming between buying extension cards with those connectors or new printers, scanner and so on altogether: either way, more money will be spent.

Note that the "buying extension cards" route is feasible only if the software components (drivers) which control the original printer and other devices *are* compatible with the new operating system. Yes, because there is no guarantee that the old operating system installed on the internal disk *will* be compatible with the new amount of memory, the new processor and extension cards and so on.

By this time, all is left of the original computer are mouse, keyboard, CD or DVD players, the disk and the case. Not bad, is it? Especially when considering that there was nothing wrong with all those other pieces, and that they would have continued to work for years, had it not been for those 88 MB of extra memory.

Of course, all this pain would have lasted much less if the "old" computer had been a laptop: they are still manufactured and assembled in so many non-standard ways, using custom components, that unless the laptop *can* handle more memory as it is, the only solution is to forget upgrades and buy a new one.

So **this** is the *true* cost, both on people wallets and on the environment, of that apparently harmless "next version of program X". Repeating the exercise for every computer of every government or business makes very easy to see the landfills being very busy with e-waste for the next few decades.

Again, please note that this true cost doesn't depend at all from the official cost or license of a program. The only things that make the difference are the hardware requirements of software programs and the protocols and formats they use to exchange data. In the first case, it is essential to develop and use software whose environmental impact, er we mean hardware requirements, is as low as possible: office productivity software, for example, could be written to run smoothly on the average computer of *three years ago*, not only the shiniest model that one can buy in stores this week. Regardless of how one plans to license or market that software.

The solution: use the right software, protocols and formats

Of course, this doesn't mean at all that society should do without software, or stop extending the adoption of digital technologies (when such adoption does make sense, of course). It is just necessary to be aware of all the risks and act accordingly.

All citizens and their Public Administrations or Schools can contribute to fight the e-waste crisis in many ways: one of the easiest and most effective ways is to make computers live longer, that is to replace them only when they actually break. This is much easier than it seems. Luckily, any computer is only as old as the software it runs. As long as that software lets you work and, above all, it is possible to *communicate* with other computer users, there is no reason to replace it.

We have already explained, however, that software can have very unpleasant effects [**3**] even if you stop using it or others *around* you use it improperly. Software-induced pollution is bad in the same way, since tolerating it on a few computers may force many others to pollute in the same way. This is especially true with Public Administrations: one single Ministry which begins requiring digital documents that can be only created with the latest version of a specific program may force all its parties to waste perfectly working computers, for the reasons described above. Therefore, besides the cultural and civic reasons we already know about [**8**], there are also health and environmental ones to demand that only truly open digital technologies are adopted.

Websites which destroy forests

Speaking of the impact of software on natural resources, one consequence of the huge diffusion of the Internet has been a great increase in the number of documents printed and discarded almost immediately, for a lot of different reasons: paper is still more comfortable than monitors for one's eyes, information like train or plane schedules must be carried along for reference and so on. In spite of this, many websites do not provide a version of their pages properly formatted for printing. They either publish their text inside unprintable movies [**27**] or seem to design pages with the explicit purpose of wasting as much paper as possible: sometimes, for each paragraph of text, the printer also spits out three or four pages of advertising, navigation menus and other stuff that one has already seen or, like the menus, is simply useless on paper.

Making available properly printable versions of each page of a website is an easy task for a competent webmaster. Restructuring a very large, already existing website is a different issue, but even in that case it is important to complain and ask for more forest-friendly websites.

Chapter 20

Does software waste energy?

Of course! Actually, this is the second big way in which software pollutes [**19**]: not only when a computer is manufactured or thrown away, but also during normal usage.

Electricity (that is, money) which enters a computer becomes heat. Which we usually pump away with other electricity (that is, money) to run air conditioners and fans.

The consequences are so serious that in September 2006 Google, the main Internet search engine, publicly called for a more efficient design for computer power supplies [**20 - 1**]. The reason? The fact that, adopting such supplies in 100 million desktop PC's running eight hours a day, it will be possible "to save 40 billion kilowatt-hours over three years, or more than 5 USD billion at California's energy rates".

Even in a single household, the energy and money flying out the windows due to careless choice and usage of computers and software programs can amount to hundreds of dollars each year. Some years ago this problem was mainly with processors and traditional monitors, now it also comes from video cards.

Some tests performed in July 2005 by a computer specialized website show that a medium range desktop computer could cost 158 USD per year of electricity [**20 - 2**] by just *being left turned on non stop.* Working or playing with such a computer every now and then could raise that cost to 230 USD per year! Note that these numbers do not include the cost of cooling the room where the computer is generating heat and the fact that computer fans, the most expensive ones excepted, are also pretty noisy.

It is true that now, at least in the specialized press, there is much more attention than five years ago to "performance per watt" that is to how much *real* work one gets done for each dollar spent on electricity. In spite of this, many people and businesses still continue (or are forced) to pollute by using much more electric power than they actually need for computing.

How to fight this waste

Turn it off

Simple things first. If computers are really so much better than ten years ago, how come they take almost the same (long) time to fire up? No wonder, then, that many people leave their computer on all the time. However, keeping a computer powered on when you don't really need it "just because", is as smart as parking your car in the driveway and leaving it on the whole night since it doesn't bother you or your neighbors. It's stupid, even if it looks very cool on a website or computer forum, to boast that you are so good at choosing and configuring software that you can keep it running for weeks, even if it is actually used only a few hours each day.

In 2005 an analysis performed by the staff of Britain's Pc Pro magazine revealed that a 50-person organization could shave 5,000 pounds off its annual electricity bill by switching computers off before leaving the office [**20 - 3**]. Of course, "if it's unused, turn it off" applies to everything electric, not just computers. Still in Britain, the Environment Minister himself pointed out in the same year that *"Britons waste the equivalent of around two power stations' worth of electricity each year"* by leaving TV sets and other gadgets on standby [**20 - 4**].

Apart from energy saving, nothing is safer for your files than a switched off computer. If you *do* have to keep it on and connected to the Internet 24/7, OK, no problem. Just pay the price, that is learn and practice the basics of computer security or pay somebody to do it for you. In all other cases, turn it off as soon as you don't need it running, or at least turn off the modem. Staying on and online is a very stupid and irresponsible thing to do if you have no actual need to do it. Switching off, or at least disconnecting any unused computer from the Internet means that, besides your own data, you will be protecting all the other Internet users. The reason is that you will greatly reduce, if not eliminate, attacks on them from *your* computer, in case it **is** compromised some day.

Use the right software

Once again, using more efficient software is the first step to save energy, or at least the easier one in many cases. Remember that, inside electronic devices, dissipated power increases greatly with the voltage and frequency of processors and other integrated circuits. In this context, efficiency is very simple to evaluate: the slowest processor that still makes it possible for you to do what you actually need to do, at the lowest possible voltage, is enough. Looking at it from the opposite angle, the software that does what you **really** need with the slowest possible processor, or at the slowest frequency, since modern processor can slow it down when they are not running heavy software, is the one that makes you waste less energy.

Separate computers from game consoles

For most home and office applications (games are an entirely different issues), the computers of five or six years ago were already overdimensioned. One of the reasons why this trend continues is the usage of general purpose computers for gaming. If you like computer games, a good solution energy-wise is to buy a separate, specialized console and only use that for gaming. The reason is that those devices, being optimized for only one task, start up much faster and are much smaller, more silent and above all more energy efficient than any desktop computer.

Demand the right hardware

More efficient computers may very well turn out to be the best real world achievement of the Children's Machine [**10**]. Even ignoring that project, it really should be much easier than it is today to buy computers which are:

- smaller and much less power hungry than normal desktops,
- unlike today's laptops, made of cheap interchangeable parts which can be mixed, added or replaced at will,
- unlike the current PDAs and other similar gadgets, flexible enough that you can install and run any software you like on them and read the same file formats as with traditional computers

The technology to make all this happen already exists: some examples are listed on the Digifreedom website. What is missing is just the right amount of consumer pressure to make it cheaper and sold in *every* computer store, not just the most specialized outlets. Please ask for a **really** energy-efficient computer or television set the next time you actually need one.

Another important thing is to look for are external devices (printers, scanners and similar) that can be completely turned off independently from the computer. If you print or scan just ten minutes every second week, why keep that printer on? In spite of this, many models have no separate power switch. Why?

Chapter 21

Does Fighting the Digital Dangers Destroy Jobs?

In order to answer this question correctly it is useful to look separately at two quite different worlds. The first is the one which consists of all those who directly make a living *today* from the current situation. Almost all these investors, companies and workers can be divided into two large classes. One is that branch of the Information Technology industry which develops and markets proprietary software. The other is the entertainment industry, or at least that part of it which produces and redistributes movies, music and so on relying heavily on DRM [**16**] and extensions of copyright as broad as possible.

Digital Dangers and software makers

Technological progress reduces the need for many jobs, no question about it. Using digital technologies which are not under total control of some multinational company, however, can have two important effects. The second one will be discussed in the next chapter. The first is helping to keep as many as possible of the remaining software-related jobs in your Country or State.

In and by itself, switching to open ICT technologies doesn't reduce the number of jobs more than the general advancement of the computer industry is already doing; it just changes the kind of jobs which are needed and makes it much easier to obtain software which is completely customized to local laws, needs and languages. If there is no need for permission or exclusive support from one (possibly foreign) company, many more *local* companies and consultants can create what *local* people and businesses really need. For the record, this is exactly what many developing countries are already doing to avoid unnecessary expenses and the risk of finding themselves in the same situation as Iceland was some years ago [**7**].

Besides that, many companies already make money out of software that can be legally installed and distributed at no cost. Some of them are even listed at the Stock Exchange. How can they do it? In practice, there is more than one way.

Some of these companies just bundle together that software with their proprietary programs, all packaged together in a way that makes much easier to install and run them. Other sell the software as part of other services: installation, maintenance, customization, training... When software is developed in this way, it creates jobs and services that may not produce dream salaries or executive benefits larger than a small city budget, but which will be much, much less likely to be outsorced: you may think of such software as a job security insurance policy for your children.

What kind of music and movies do you want?

There is no doubt that some kinds of extremely expensive movies, TV or live shows, as well as most worldwide merchandising campaigns are only possible with the current economic model of entertainment industry. There is also no doubt that a lot of great literary, musical or film works are so great and see the light only because a lot of competent professionals, from editors to special effects or make-up specialists, could be paid to work full time to assist the authors and artists who all too often are the only ones who become famous.

But if producing a blockbuster costs tens or hundreds of million dollars; if only one out of every ten blockbusters is profitable; and if there **must** be at least five blockbusters, albums or live tours per quarter with six digit profit figures, not because the public wants or needs them, but to make a few stock holders happy, then it is no surprise that the most popular movies always come from a handful of big movie and music companies. Financial efforts on this scale are possible and justifiable only if those who undertake them are sure that they can monopolize all profits for decades by successfully suing, just as an example, everybody who:

- independently produces entirely new and original stories with the same characters
- reuses more than one second at a time of any music, movie scene and so on which already exists.
- produces T-shirts or anything else with slogans, drawings (not logos, that's a different issue) or anything else remotely resembling something which already exists
- tries not to pay for the same thing twice, for example copying a regularly purchased VHS movie on DVD to save shelf space

and so on, regardless of how, and to what degree such "competitors" will ever be profitable or how many real world losses they will cause for those who did or *financed* the original work.

Therefore it is very likely, if not almost certain, that in a world with a much shorter copyright duration and really fair regulations on reuse [**15**], format or time shifting [**14**] and similar issues there would be many fewer pop stars a la Britney Spears or James Bond movies. In such a world it would also be possible to purchase or obtain every music, movie or book more than a few years old from many independent sources, that is, at the smallest possible cost.

What about job creation and making a good living only out of artistic talent? On one hand, there would be much less space to make huge amounts of money by just being *intermediaries* or *"assistants"*, in the largest possible meaning of the word, of the actual artists and authors. At the same time there would also be many more possibilities than today for starting and running many collateral businesses, from repackaging and distributing older works to selling ”special editions” for niche markets. The effects of a more balanced system on beginning, independent artists would also be much, much less harmful than on the Top Ten pop stars of today, and it is very likely that most of them would benefit (if copyright were reformed, but not abolished of course!) from it.

Everybody, parent or *citizen* should decide for his or herself whether this is a bad thing or not. What is important is to decide as soon as possible, before all roads are locked beyond return [**17**], and act accordingly.

Chapter 22

Would all the other businesses and jobs suffer from fighting Digital Dangers?

The second reason to fight Digital Dangers just in order to *boost* the (local) economy is to make it much more affordable to start up and run a small business in any field. For an artist, fighting the Digital Dangers makes it much easier to live off the profits of his or her own talent, be they from copyright or other sources, with much more control than is often possible today.

In all these cases (basically, everybody on Earth but large corporations and artists who have **already** won three or four Oscar or Grammy Awards) the difference between open digital technologies or balanced copyright models and the current situation is the same as between owning a house and renting an apartment. If you are the owner you, not the landlord, are free to find and choose the best contractors who will remodel the house like **you** want, **when** you want and at the best possible price. All without any need to become an electrician or a plumber yourself. And there is no risk that somebody blocks your access to the personal files, er, belongings, that you left inside the house because *they* decide that it's time to remodel or double the rent.

Freeing small businesses from software hassles

Truly open digital technologies can create or save a lot of medium and small businesses, sometimes even outside of the programming sector.

In August 2006, for example, many Internet cafes in Malaysia were informed that letting their own customers use the software purchased for the store [**22 - 1**] was not permitted, unless they purchased a different, obviously more expensive license. The basic license of many commercial software products allows their use only by the employees of the company which purchased the license.

The cost of the license was still too high, and wasn't even a one time fee. After a quick investigation, many of those Cafe owners discovered a much cheaper and safer alternative [**38**], one that may be useful for many other small businesses in any part of the world.

In many other cases software free from high licensing costs and complicated end-user agreements may be the only way to start up or run any business with peace of mind. According to a January 2007 report, small and midsized businesses are often more at risk than larger ones [**22 - 2**] of being investigated and sued for software "piracy" issues. Even if they still *"have got the original disks, packaging materials and registration documents all on file"*.

Will the Internet work against small businesses?

The Digital Dangers for small businesses don't come only from how *software* is priced or licensed nowadays. Unbalanced implementations of Net Neutrality [**9**], for example, may hurt small companies and start-ups much more than large corporations.

Another trap lying behind the corner for all small businesses may be the anti fraud feature built into the most popular proprietary Internet browser [**22 - 3**]. This is a problem especially for all those activities which were impossible, or much less profitable, before the Internet.

Internet Explorer 7 will be the first browser able to color in green the address of genuine websites and display their owner's identity. Note that displaying "www.acme.com, owned by Mr John Doe" in green only means that the website you are looking at *is* the one actually run by Mr. John Doe. It is no guarantee at all that Mr Doe is an honest guy.

The same browser can also turn Internet addresses yellow on suspicious sites and red on sites which have already been confirmed as fraudulent. All the websites for which there is neither good or bad information would remain plain black on white.

Regardless of how many browsers support it, once this system really takes off, many consumers will naturally feel that it is only safe, or much safer anyway, to only shop on "green websites". So far so good, but for small businesses this has already been defined by an expert as *"a ticking time bomb that is going to explode"*.

As they are conceived today, the green colors only appear for websites which have received a special certificate from a central authority. The trap is that, at least initially, sole proprietorships, general partnerships and individuals won't be eligible to apply for the certificate, no matter how honest and trustworthy they are. The members of that authority couldn't agree on which rules to apply to such businesses.

Managers sealing theirs and every other company inside a casket

We have already seen how much DRM hurts honest citizens, reducing their acquired rights **[16]**. This by itself would already be a serious problem, but there is another face of DRM, entirely confined to the workplace, whose effects may be equally harmful. Access and copying can be forbidden or restricted on any kind of file, not just those containing music and video.

The latest versions of some commercial operating systems, office suites and directory services can provide private companies and Public Administrations with much more advanced ways to secure their data than in the past. Using these technologies, theft or involuntary leaks of confidential documents (even among different offices *of the same organization*) could stop or, more realistically, happen much less frequently than they do today.

This is important because, according to the American Privacy Rights Clearinghouse, the total number of data breach victims has passed 100 million **[22 - 4]** since they began tracking in February 2005. The theft of one single Boeing laptop in January 2007 left in still unknown hands unencrypted information on 382,000 employees **[22 - 5]**, including Social Security numbers, home addresses, telephone numbers, birth dates and salary information.

When hearing of such accidents, better data protection systems sound great, don't they? Which manager would be so foolish as not to jump at this opportunity? The only problem is if these technologies turn out to be another one way street that makes it practically impossible to change software supplier later on, even if it decides to increase its prices tenfold.

Consequently, even in this case, the choice is easy. There are just two questions every citizen or business owner should ask the provider of their "data protection software" about this:

- can I get out next year, that is can I still access and protect all my **own** files in the same way if I decide to change software?
- if the Public Administrations we all pay with our taxes adopt these systems:
  - will small, local companies still be able to afford the expense to exchange documents, that is to still make business with them?
  - will private citizens be able to communicate with them via computer with the software they prefer, even if they cannot afford the latest computer models?

In a nutshell: regardless of the price of some software, adopt it only if you are sure that you can leave it tomorrow without suffering. According to some experts, today many public and private organizations could already switch 80 per cent of their users to alternative software systems much easier than ever before [**22 - 6**].

The training myth

One obstacle to switching to new software programs is the perceived cost of training or retraining themselves or one's employees. Many of us would probably be very happy if there were only two or three types of immutable computer programs to learn [**7**], even when the differences between the "familiar" software and the others are just the color or the position on the screen of some icons. Very often however, the official reason to not even consider changing from the current software sounds much more professional: *"One license of the software we already use is X dollars, while a training class for new software costs twice as much, plus three working days lost: where is the business case?"*.

The first obvious answer is that, at least in Public Administrations, there may also be cultural and political reasons to justify migration costs [**7**]. In the second place, once off costs should not be directly compared to annual or otherwise recurring ones, but let's spend a few words on this (re)training myth.

Very often, at least in offices, there is no need to replace the whole software environment overnight. The OpenOffice.org [**22 - 7**] office suite, for example, has no license costs and is more than enough for most documents, presentations and spreadsheets. Of course, it doesn't look and feel *exactly* like the most popular one, but is this enough to require a full time, multi-day migration course for people who already are computer users?

For basic usage a change of software could even go unnoticed; for expert users, unless they really, really need some **function** not present in any other product, complaining about a switch may be ridiculous. This is the Third Millennium, isn't it? The age when a modern office environment, word processors and spreadsheets are the really basic tools that every employee should know, just like for pens and pocket calculators. Do you schedule training when you start buying pens and binders from a different stationery shop?

Also note that retraining is an issue only with users who have *already* spent a lot of time and energy becoming familiar with something. For people who are *starting* to use computers, it really doesn't make much of a difference which software they start with. Should kids be given rotary phones only because everybody over 40 spent most of his or her life with these instead of keypads? Obviously not.

The solution to minimizing training expenses or avoiding them altogether is simple: just use digital technologies which are really interoperable [**40**] and, as far as communication and team work are concerned, most problems simply disappear. Everybody can work with the computer and software he or she has available, ignoring what the others use. Yes, in medium and large organizations this may imply an higher support cost, but it would be a temporary phase.

Chapter 23

The tax on future, alleged guilt

The hidden cost of software on all citizens, including those who don't even use a computer, has been already described at the beginning of this book [**3**]. In addition to all that, there is another tax forced on all students, families, schools and businesses from the entertainment industry.

What's in the price of most digital devices

Since all bits are equal [**1**], today it is possible to store any data, including music or movies, on any object which is able to store bits. This fact of life causes all families and companies to spend more than it's necessary on digital devices and media, without even knowing where all the extra money goes. Here are some examples.

In November 2006 Microsoft announced it had agreed to pay Universal Music Group (UMG) a portion of the revenue from sales of all its digital entertainment device Zune [**23 - 1**].

An anti piracy law presented in Sweden in 2005 included the proposal to triple the price of blank DVDs [**23 - 2**] in order to guarantee "proper payment for their work" to musicians and film-makers.

For the same reason, Canada has a 21 cent levy on every blank CD media and a 77 cent one for each for CD-R Audio, CD-RW Audio and MiniDiscs. In February 2007 the Canada's Private Copyright Collective asked for an 8 cent increase of these levies [**23 - 3**]. Besides that, and always as a way to "compensate artists for unauthorized copying of their *music*", the Collective also proposed several levies on any digital recording medium, from 2 to 10 dollars on each of the memory cards used almost exclusively to store *pictures* in digital cameras, to a 26 per cent increase (from 290 to 365 dollars) on the street price of music players like the Apple's 30GB iPod.

In 2005, the cost of a CD-burner in Germany included 7.50 Euro of compensation for illegal copying: the levy on blank CDs was 9 cents and 17.4 cents for each blank DVD. According to a Rightscom report quoted by the International Herald Tribune, in 2004 alone the consumers in Germany, France, the Netherlands, Italy and Spain paid 542 million Euros of fees of this kind [**23 - 4**] on everything from copying machines to TV set-top boxes.

A few years ago VG Wort, the German collection agency for copyright fees, asked for a 30 Euro levy on each new *computer*. Cell phones which can also play music are next in the list in several countries, as well as the hard disks used to store data in every computer or fast, flat-rate Internet connection used to download files from the Internet.

A huge step back in the legal system

Today levies like the one described above exist, in one form or another, in most countries of the world. Especially in Europe, as the public policy director of the Business Software Alliance put it in 2005, there is a system of semi-autonomous collection agencies "that are no longer responsive to public opinion or pressure" [**23 - 4**]. The result is that some hardware companies have already decided in the past to *not* sell some of their most economic music players at all in some countries: the percentage price increase due to the levies would have made those products too expensive for their target market.

The damage from copyright levies on the hardware industry is not to be undervalued, since it *may* indeed lead to fewer jobs in that sector. Equipment and hardware manufacturers, however, officially are in favor of "replacing levies... in the digital environment" [**23 - 5**] with something that may be even worse, that is DRM [**16**].

Besides that, the main reason to worry about this particular Digital Danger is that it costs a lot to all families with a motivation and in ways that, regardless of how much money is involved, are absurd, really unjust even in principle and, in practice, impossible to apply according to their official purpose.

The basic assumption behind all these levies is always the same and remains unbearable: **everybody** is "guilty unless proven innocent" or, more exactly, "surely guilty", so he or she must pay in advance for their **potential, future crimes**.

This is similar to sending **everybody** who buys a bottle of liquor or a car to prison, **the day they buy them**, because statistically they **do** have a probability of getting drunk and killing somebody some day. Such a principle is exactly the opposite of what is practiced by all the civilized legal systems in the world: if anybody tried to apply it explicitly, rather than through levies on digital devices by semi-private, almost totally autonomous agencies, he or she would be in serious trouble before any Court, or at the next election.

Of course, there is no doubt that copying beyond fair use or unauthorized redistribution of music, movies and so on is illegal and unfair to the creators and performers of those works [**18**]. It is also undeniable that there are too many people, especially younger ones, who use computers, music players or DVDs mainly to store and play illegally copied materials, hiding behind noble-sounding repetitions of ideals which they don't really understand or care about [**34**].

Does the money go to the right people?

Even ignoring the huge ethical issue above, however, the levies are and will remain impossible to apply in a rational and fair manner. They totally ignore fair use and format shifting [**14**] of legally purchased material: if you want to make a backup copy of a CD bought at the store on your computer and portable music player, nobody will reimburse you for the levies paid three times over the same song (on the CD, the computer and the portable player).

It is also impossible, both technically and in the interest of privacy, to know which devices will be used for illegal copies and to what extent. People who just want to save their home movies will pay blank DVDs the same as those who never buy or rent an original DVD at the movie store. The computers purchased by companies, for internal use, or those bought (on budgets which get tighter every year...) by schools for their labs can be easily secured or monitored to prevent illegal copying: are they exempted from the full levy?

Next, paying the levies doesn't even cancel the crime of illegal copying in many countries. People who pay these "artist compensation" taxes on new computers and CDs but then store copyrighted music on that same equipment will still be sued by recording companies if the latter find them [**13**]. On the one hand, this may look like the proper reward for fighting a stupid system in a counterproductive, even stupider way [**18**], but this doesn't make the levies less absurd or harmful.

The other huge practical and ethical problem in the levy system is the total lack of transparency and/or fairness in how the collected money is distributed. It is impossible to know how many times each existing song was or will be illegally copied, that is to know how the livies should be divided among artists. No problem: a generic *recording company* will always get the same part of the levy on each portable music player, even if the person who purchased it will never, ever listen to, or copy illegally, any music distributed by that specific company.

On the other side of the wall, small companies or all independent artists who cannot or do not want to be part of the cartel are simply left without money. Only those who *already* are under contract with a multinational *and* in the Top Ten list, that is those who have *already* made a lot of money anyway, are sure they will get a meaningful slice of the cake.

The only reason why this has gone so far is because the price increases are not spelled out in plain sight. From this point of view, it could be really useful to mandate by law that the price tags of every digital device or storage medium specifies how much of the final price is a copyright levy.

Chapter 24

The Digital Troubles of politicians and the Military

What do a UK prime Minister, a US warship and a fighter plane have in common? They all were put in danger, or at least in quite embarrassing situations, because of poor design, use or understanding of software, or at least of the policies that should regulate its use.

In 2003, the British Government published online an official dossier on Iraq's security and intelligence organizations [**24 - 1**]. Most of that dossier had been simply copied from three different articles: after a quick, very basic analysis of that file, a security consultant was able to find out who had worked on the document [**24 - 2**].

On June 16, 2006 negotiations between the United States and England for a very advanced military plane, the Joint Strike Fighter, reached an impasse [**24 - 3**]: England, being a sovereign State, obviously wants to be able to maintain its military airplanes without relying on any foreign contractor. In order for this to happen, one of the necessary conditions is to have unlimited access to the source code [**37**] of the software which controls all the vital functions of the plane, from flight control to communications.

Consequently, in December 2006 the British Ministers were urged to start searching for alternatives [**24 - 4**] to the 140 billion pound project unless the United States "agreed within weeks to share sensitive technology". Such worries are not just theoretical. In 1998 the USS Yorktown remained "dead in the water" for more than two hours [**24 - 5**] because its computers were unable to divide by the number zero. It took two days of pierside maintenance to fix the problem.

Some of the problems mentioned in this chapter come from relying on what the specialists call "security through obscurity", an approach whose validity seems very limited today. Security through obscurity is when any company designs a weak (security-wise) product for any sensitive application and then keeps the design a secret to hide the flaws and limits, while marketing it as unbreakable just because of that secrecy. Conceptually, this is the same thing as using a cardboard door for your house, placing a big plant in front of it and then feeling safe because thieves and other crooks "won't be able to find where the door is, ah-ah!!"

The truth is that, no matter how many extremely competent engineers in one company develop and maintain the product full time, there will always be one million times that many programmers around the Internet to break the code very soon. It might just happen by their sheer numbers, like the story of one million monkeys dancing on one keyboard, and eventually producing by pure chance a Shakespeare sonnet.

Really open formats and software, especially when national security is concerned, could be of great help in all these cases. The doors of bank vaults are not made of tempered steel because nobody knows what steel is. They are made of such materials just *because* every expert knows their composition and consequently *can* confirm that it is the best possible one for the job.For the same reasons, security software developed in the open would have much a better chance of being resistant to faults and intrusion attempts: were such weaknesses present, any expert could have the possibility of finding and denouncing them. Software chosen in this way would also have the extra advantage of being legally supportable by many different (local) software companies, thus giving the Government more negotiating power when choosing a supplier, more opportunities to create local jobs and less ways to waste your taxes.

Of course, the effectiveness of such solutions would be limited without correctly formulated laws and procurement contracts together with, as desperate an effort as it may seem, a proper ICT basic training for all government officials and Parliament Members.

Chapter 25

Is E-Voting a solution? To which problem?

E-voting is coming, or has already arrived, in my Country. How can I understand if it's implemented properly, without risks of abuse? What is the right way to e-vote?

Let's start with the real question that almost nobody asks: is e-voting necessary in the first place? Does it really makes any sense at all?

In order to understand which problem(s) e-voting should actually solve,what is real cost is and how things are going now, we will now shortly review the main justifications presented for e-voting, and then look at some reports from the trenches.

E-Voting is good because...

....it stimulates people to vote

Nice start. Did you realize that they are insulting you, by treating you like an infant? "Bobby will eat his peas quietly if the TV is on"! Do they think you can't hold a pen? Why aren't you voting? Is it really because a pen signature on a sheet of paper is oh so much more boring (or difficult) than placing a finger on a monitor? Or is it because all the available choices are equally depressing, wherever you read them? People who don't vote because it's boring have bigger problems, and probably deserve anybody who is elected thanks to their absence.

Said this, even if gadgets were really a solution to low voters turnout, there is no doubt that scratch-n-sniff stickers or Playboy calendars would be a much more effective, cheaper and safer solution than any untested technology.

....it reduces voters' errors

See the comment above on placing a finger versus holding a pen. Anybody who seriously believes this has never stopped one second to compare the number of people who can still write a simple note without assistance to that of people who still stare at a computer screen. Pen and paper are still immensely more familiar and less intimidating than computers.

....it reduces counting errors and frauds

Too many young peoples are unable to count properly [**25 - 1**] and part of the fault is just the misuse of computers [**10**], but we digress. Sure, humans make many more errors than computers when counting manually. But it only takes one flaw in the computerized booths, or one person rewriting their output remotely, to alter many more votes, much more quickly, than if humans were doing the job and checking each other's results. If vote counters are humans, you have to corrupt or menace many more people to steal thousands of votes and get away with it.

... it's much faster

How often will you be called to vote in the next ten years? Every day? Elections of Parliaments, Presidents, Majors and similar normally take place every two to five years. A country without e-voting, but with a decent procedure will know the result, without ambiguities, in a couple of days anyway. If this doesn't happen, there are problems that no e-voting could fix. What is the difference between knowing the new President four years and two days after the previous election and knowing him or her four years and two *hours* later? How can you justify rebuilding the whole system from scratch to gain about one day every few years?

... it saves money

Sure. A lot. Enough to fix the whole country deficit, no question about it. Like we just said, how often will you be called to vote in the next ten years? Please take all the money spent to count votes in the last election without e-voting and divide it by the whole State budget between two consecutive election. The percentage savings would be greater if we just switched the light off every time we go to the bathroom. Any savings caused by e-voting would be much smaller than the dangers it creates. If you don't believe this, just keep reading.

E-voting nightmares

In July 2006 in Sacramento experts found what may be "the worst security flaw we have seen in touch screen voting machines [**25 - 2**]". They reported that, having access to these machines, it would be possible to completely rig an election without leaving a trace.

In august 2006, election officials reported that some machines were causing difficulties in several counties of Nebraska because they were not set up properly [**25 - 3**].

In the same month, voting machine failures stroke again in Alaska [**25 - 4**]: they forced elections officials to hand count and manually upload vote totals [**25 - 5**] from several precincts across the State.

In September 2006, other tests found out that Hotel Minibar Keys can open voting machines [**25 - 6**].

In October 2006, Canadian columnist Michael Geist analyzed the status of e-voting [**25 - 7**] and concluded that *"the reliance on Internet and electronic voting may inadvertently place the validity of the election process at risk"*.

These are just a little part of the many proofs that this technology isn't mature enough to be trusted. More examples and other information on e-voting are on the Digifreedom.net website.

Why banalize voting?

Even ignoring the practical problems, the whole concept of e-voting is quite depressing, really. In our culture, we still place much more importance in signatures on papers than in shiny computer monitors. Most people still look at computers as mere gaming stations, fancy gadgets or, in the best case, super typewriters: not really relevant stuff.

Voting is a privilege and a achievement. Reducing it to an arcade game is dangerous for democracy. It sends the message that voting is just like going to a soda vending machine, that is not important (just what the establishment would like us to think, isn't it?). When we have to put something on paper, instead, we take it much more seriously. We think about it first. This is how voting should remain.

Is there a solution?

Yes. Do without e-voting, because there is no meaningful reason to adopt it yet. Some activists say that e-voting is a good thing, as long as it is done with software which is Free as in Freedom [**38**], software that everybody can check without restrictions. The Open Voting Foundation [**25 - 8**] promotes just the adoption of this way to e-vote worldwide. There is no doubt that, if computers must replace paper in the voting booth, the whole system, both hardware and software, must be as transparent as possible: as far as software is concerned, Free Software would be the only way to go for e-voting.

This said, promoting e-voting just because it can be done with Free Software continues to not make sense. If the software running the system were open it would still not solve any of the problems listed above, or give citizens any meaningful advantage.

In the real world, having the source code **[37]** of a voting machine would change nothing at all at the voting booth. 99% of voters would not know what to do with it anyway, and what should the rest do? Block everybody else in the line for 30 minutes, while he or she checks the source code in the machine against the copy in his or her pocket? Or disassemble the machine to check that it was not modified to hide that it runs the wrong software? Come on!

Actually, e-voting could even make thing worse, *decreasing* the guarantees that counting is done without frauds. With paper, almost everybody has the skills to be an election official and figure out in real time (like any voter standing by in that moment) if somebody hid one ballot paper under the table, or declared it contained one more vote for his or her preferred candidate.

In this sense, e-voting may even be anti-democratic, a very elitist thing to do: "only citizens who can program are good enough to supervise the exercise of democracy"? No, thanks.

Chapter 26

Can freedom of speech and participation be actually practiced?

You may have heard of absolutely ordinary people, with no special talent or worthwhile stories to tell, keeping an online diary. The original name of these personal online journals was *"web log"* but, since the original form is so long and hard to remember, the name was shortened to *blog*.

This kind of "publishing" is the latest fad made possible by the abundance of relatively cheap computers, software and Internet connectivity. This has three big effects at the social and cultural level.

The first is the reality show of your worst nightmares come true: billions of terribly written (but in real time, mind you!), extremely boring web pages. Apart from how much this stuff pollutes the result of Internet searches, ignoring them is very easy.

A second, more serious problem, is how easy it is today for people to hurt themselves or harass others on a large scale, violating privacy or damaging one's reputation. We have already seen how this is not a theoretical risk [**5**], but something which requires both technical and non technical solutions [**42**].

The third, large scale consequence, which makes it worth coping with the first two problems, rather than just giving up the whole concept of personal computing, is very simple to describe. For the first time in history, freedom of speech and efficient civil action are easy, inexpensive (if one can afford a computer, of course) and everybody can practice them for real. What was, until today, a right written into some Constitutions but not a practical possibility is now actually feasible: everybody can denounce wrongs, start a political party or a civil rights campaign reaching many thousands of people with very little money.

Consumer revolt

A good reason to have a home computer and above all to learn how to use it properly is the possibility of having much more control than in the past on how much money others can force you to spend. This happens when many thousands of people coordinate their actions through the Internet, and is not a theoretical possibility: in the United Kingdom alone, 4 million householders have dumped their utility suppliers and found better gas or electricity deals after an Internet-led consumer campaign [**26 - 1**]. British Gas, for example, slashed gas bills by 17 per cent and electricity bills by 11 per cent in February 2007, after losing more than one million customer in the previous year, thanks in no small part to such pressures. Large scale civic actions on everything, from planning applications for superstores in sensitive areas to excessive bank fees, are already managed in the same way, with the smallest possible amount of money and time for all the campaigners.

Of course, the Internet itself isn't enough to make such things happen. One real, hand signed letter or fax, not to mention face to face meetings, can still accomplish more than one thousand email messages, but computers and the Internet make immensely easier to collect the necessary information and coordinate the individual efforts of many people. The sooner *all* parents start to use a home computer in this way, the better for their wallets and their children.

Discovering (finally!) how your money was spent

Using a family computer in the right way doesn't saves just the money spent on private transactions. In 2006 two USA senators proposed a bill to create a searchable database, as simple to use as a normal Internet search, of the trillions of dollars spent every year on government contracts, grants, insurance, loans and financial assistance [**26 - 2**]. Imagine that: being able to know in a few minutes how much was actually spent and how in your State or County on each budget voice. Without filing forms, wasting time, asking for permissions or even leaving your house. Can you imagine a better reason, even for those millions of seniors and other average citizens who don't own or regularly use a computer yet, to change their habits and spend some time online doing something useful and interesting?

It would even be another boost for the computer and Internet industries, wouldn't it? There are many people who still see no reason to spend time online or "sharing" movies and music.

An online database of Federal Government spending [**26 - 3**] already exists in the USA but, according to its own managers, it is *often missing parts or sections and at times is significantly limited in its usefulness... solely because of the way the government collects and manages the information."*

Right now, that USA bill has been stopped, but the opportunity remains: hopefully that bill or similar ones will pass soon, in the USA and any other country, making for the first time civic participation and scrutiny on a large scale a reality. In order to accelerate this process, of course, it is essential that as many people as possible demand and **use** exactly this kind of access to public records.

Your digital license and registration, please!

What is the first consequence of this active citizenship paradise? It's obvious: now that freedom of public speech to a huge audience is both technically possible and cheap, here come the laws to make it illegal unless you have the same pockets and connections as in the past.

Why not? There is no reason to not let freedom of speech and other rights continue to be officially granted in Constitutions when, from stopping bills like the one above to anti Net Neutrality legislation [**9**] or turning copyright into anti-documentaries weapons [**15**], there are so many legal ways to make them practically and economically unfeasible to newcomers.

Of course, to be taken seriously any (for lack of a better term) ”online civic journalist” will almost always have to make his or her identity known and, in any case, accept full responsibility for what he or she publishes. These, however, are requirements which do not imply, nor can they justify in any way, the imposition on private citizens of the same fees or regulations which were made for nationwide newspapers with full time staff. If the laws of your Country already give you freedom of speech, that's enough. You don't need certificate or badges to practice your basic rights online, just because you can reach more than ten people at a time in that way or because your reports and opinion pieces may decrease the readership, that is the profits, of some established newspaper.

This is the danger to avoid: before voting next time, it will be important to ask to all candidates which regulations they think proper for self-supported, single ”online civic journalists”. If they think ordinary citizens should pay some fee or pass some bar examination to keep the rights they already have... the conclusion is obvious, isn't it?

Chapter 27

What Is Web Usability, And Why Should I Care?

Some websites may look very cool at first sight, but in practice they are unusable and a big problem for everybody. Some web publishers, for example, transform material like photos, articles and stories, which are **not** movies, into movies viewable with web browsers, that is the same software programs used to read normal web pages. The two most frequent reasons for this behavior are fashion and paranoia: some web publishers need to look as flashy as possible, in the illusion that this will convince more people to visit their website regularly. Others believe that all that effort will actually prevent illegal copying of their material.

The result is websites which are as practical to use as giving people, instead of a book, a videotape or a DVD where somebody holds the same book in front of the camera and turns the pages to let you read them. Such solution are much less usable than the original format: people have to read slowly because it takes more effort to download, and maybe need to buy a computer powerful enough to handle the movie version. The same applies to pages full of unnecessary decorations and images. Remember that the great majority of the world's population (including a lot of people in "developed" countries) still has to work months or years to afford a computer. Even the others don't really like to be **forced** to spend money without an actual reason. Besides this, Internet search engines (the websites which try to index all the content of the Internet) have much more difficulty in indexing text hidden in this way, so these websites are more difficult to find, and much less useful as marketing tools.

Next in the race for the "Website clients-who-don't-get-it" Award come those websites owners who require or tolerate web pages which can be viewed well only with one model or version of browser, or for a certain resolution of the monitor. Such an attitude is just as smart and polite as saying "I'll sell you this book only if you promise to read it when holding it exactly ten inches from your nose, even if it's uncomfortable for your eyes or your arms are tired": this flies right in the face of the Internet as a unifying technology. A website designed in this way is invariably optimized only for *some* of its potential users.

Another class of Internet stupidity consists of those websites based on brain-dead color adjustments like black text on blue background. Oh, and what about all the introductory commercials which plague many websites, wasting a lot of people's time? Websites are not television: most of the time when you follow a link or type an Internet address it is because you already have a good idea of what you will find. There is no reason to waste your time (or your money, if you are on a metered Internet Connection) with a mini-movie which takes much more time than text just to reach your computer. Everybody skips commercials: the only reason why many organizations and businesses pay designers for these introductions is they haven't' realized yet they are just that, expensive commercials which are very easy to skip, when not harmful because they bore potential customers.

Last but not least come those online stores which, by default, make your computer automatically play *their* favorite background music, ignoring the fact that people coming to their website from the office, or when kids sleep, will most likely not come back.

Making any of these mistakes may nullify all the time and money invested in a website. All these so-called "richer user experiences" were already a problem in 2002, when the report "A Fresh Look at Internet Speed" **[27 - 1]** denounced that the load caused by all this eye candy was just too much for low speed Internet connections. Today this is still true. Bandwidth is still limited and expensive in many cases, both for websites and their users. Flat rate fast connections are still restricted to a few parts of the world, and those areas are usually the same where metered Internet access from (cell) phones and other portable devices is catching up. Regardless of speed, what about small displays or, much more important, disabled users? Ignoring usability can be OK for small, mostly private sites, or entertainment and game portals which would have no reason to exist if they could not sport every multimedia trick in the book.

The majority of websites, instead, that is all those which are theoretically meant to sell something or provide information and service to the greatest possible audience, should avoid all these mistakes like the plague.

Websites remain useful and usable (even as a marketing tool for small businesses) only if they take real people - all of them - into account. Real Web accessibility for disabled users is also becoming essential for any commercial website, if nothing else because its absence can bring lawsuits to your business: very recently, even a giant like the Target chain of department stores learned this the hard way [**27 - 2**].

Chapter 28

Does it make sense to buy a computer and not install software on it?

There is a way to do something useful with a computer which is pretty trendy nowadays: Application Service Providers (ASP). These are companies which install and set up software programs on *their* computers and then let you use them through the Internet, normally inside a web browser. The most popular category of software of this kind is online office suites, that is Internet-based systems to write office text, spreadsheets and presentation.

ASPs normally make money either placing advertisement in the browser windows or simply charging their users a monthly fee. In this way, home computers become very little more than a long extension cord connecting the monitor and keyboard in one's living room to the remote computer where all the action takes place. Ordinary people just use the programs, somebody else spends his or her time figuring out how to install, configure and maintain them up and running.

The selling point behind this and many similar trends is the question "When it comes to computers, who do you want to be, a user or a programmer [**43**]? Can you afford to be both? Why should you? Let **us** do the dirty job for you. Don't waste time and money to buy, configure and maintain expensive computers and software. Just use the programs you need and be productive **now**, for heaven's sake! Who cares if you're doing it through a web browser?

Installing all the software only on one central computer which acts like an ASP, so that all the employees or students cannot alter it, is the standard way of working of many organizations and, indeed, a smart thing to do in those scenarios. This is because the users of such ASPs are all in the same building or closed network, very close to the central computers, not on the other side of the Internet: it is very easy to work more efficiently, reduce maintenance costs and still guarantee reliable operations in such restricted environments.

Outside closed organizations, that is when it is offered as a service to the general public, the ASP way of working makes still sense in many situations. Other times, however, it just looks like the Internet-enabled version of *"don't worry, and don't bother to understand, just give us all the money we ask for"*. Of course, you have to focus on your core business, and who dares being caught out not doing that? What would mommy say?

Almost all of us are not programmers, nor have any need or interest in becoming one. From this point of view, freely giving some money or attention to somebody else, so you can keep doing what you know best does look like a wise move, and in many cases it may actually be so. There are also many cases, however, where the contrary is true.

When running a business, especially a small one, outsourcing bookkeeping and tax returns to an external certified accountant is probably a smart thing to do, because fiscal law has been made so complicated that almost everybody faints just being close to a manual.

When it comes to things that you **must** do yourself as soon as possible, however, things can be very different. Here are some cases when, if you have to do something with a computer, you do *want* to have all your hardware and software in front of you, not in some vault many miles away:

- when Internet connectivity is not guaranteed
- when you need decent speed: in real world conditions, it only takes one slow computer between you and the ASP to slow down everything you do
- when being forced to work with a reduced user interface [**28 - 1**], in a small portion of your monitor doesn't really slow you down
- when doing really basic or simple things that you need to do repeatedly. What would you say, for example, to somebody suggesting "Here, don't bother learning how to read, write, and multiply by ten, I'll do it for a fee, so you can focus on your core business..."?
- whenever privacy matters. Using a remote ASP as if it were your computer means you have to trust it enough to be sure that your personal files are not handed over to somebody else [**5**], and that nobody else is eavesdropping.
- when you are a Public Administration that must keep complete control on all its data and guarantee that they always remain accessible, since they belong to **all** citizens!

Chapter 29

Is it right and technically possible to block or restrict Internet Access?

How The Internet is blocked in some countries

When it comes to whole countries, censorship has always existed, but the Internet makes it much harder: the quantity of information to block is immensely greater than in the past, and much of it is usually published from computers abroad, which cannot be shut down. There are several partial solutions to this: one of them may be to make it easy, or possible, to surf the Internet only from public computers, as happens in China [**29 - 1**]. Other methods to limit Internet access from Chinese points of access include canceling some addresses or domain names from the lists of known destinations or redirecting them to other websites. According to a study of the Open Net Initiative (ONI) [**29 - 2**], Internet filtering in China in 2004 was already based on multiple levels of legal and technical control. Thousands of websites were blocked in this way, and not only those containing pornographic material: even University websites, as well as health or news portals were filtered. The Maxthon Web browser has become very popular in China just because it makes easier to bypass some of these restrictions [**29 -**

3].

Censored topics in other countries also include web diaries and pages addressed to linguistic minorities. ONI also released a report about increased Internet censorship in Vietnam [**29 - 4**]. Similar things have been documented in Saudi Arabia [**29 - 5**] and Iran [**29 - 6**].

In Europe there are proposals since 1999 to "promote safer use of the Internet" [**29 - 7**] through an Action Plan which should be part of "a coherent set of policies at EU level to deal with illegal and harmful content on the Internet".

Who makes this level of censorship technically possible?

Some of the countries mentioned in the previous paragraph, as well as several western nations rely upon commercial software developed by for-profit western companies to perform filtering. Back in 2005, Iran acknowledged that it outsourced many of the decisions about what its citizens can access on the Internet to a United States company, which in turn profits from its complicity in such a regime. Ignoring for a moment the democracy and free speech issues, a basic problem here is that the software used, being out of the control of its user (the Iranian Government) is prone to over-blocking, errors and lack of transparency.

Is it right in some situations? If yes, when, why and how?

Indiscriminate, government-mandated blocks are wrong, no question about that, and assuming they can actually be enforced on a whole country for extended periods of time, is pretty much naive.

The situation is somewhat different when minors are involved and/or the computers and Internet connection have been provided and paid for for some specific task. This is especially true with computers provided by schools: blocking access to websites devoted to games, adult material, online chat rooms and so on, is really something you can and should ask for without any fear of looking old, out of the Ark, oppressive or narrow-minded. In those cases there is nothing to discuss: filtering access is done to save time and money. No distraction on study time paid by family or the State: Freedom has nothing to do with this, it's just a matter of efficiency.

The only risk in this case is when you don't take charge and responsibility. If you approve or require restricted Internet access for your children at home or in their school, for example, **you**, or somebody you know, trust and can actually control, have to decide what is admissible and what must be blocked. Nobody else. Practically speaking, this means using Internet filtering software that lets **you**, or your delegates, write the whole blacklist. The Digifreedom website lists some software tools that give you this freedom.

Chapter 30

Is that really you?

In a digital world, complete and real anonymity online is a mere illusion unless you take a lot of steps, including several ones which may very likely be illegal or not allowed by the contracts offered by any Internet Access Provider. Even in that case, there are many occasions where *you* will want or need people online to know who you really are. Occasions, that is, when **you** will need the capability of demonstrating online, in order for your everyday life to work smoothly.

In a few years, the capability of having and proving an *online identity* could become really necessary for travel, to obtain a bank account or credit card, apply for a job, activate utility contracts or other services and so on. In all these cases, everybody would save a lot of time and worries if even online it were possible, fast and easy to certify the online identities of all the involved parties.

Until this day, we have all more or less managed to carry on with passports, ID cards and driver licenses made of paper, for the simple reason that we didn't need to show them to somebody sitting in front of a computer thousands of miles away from us. The fact that we are moving, whether we like it or not, to a digital and digitally managed world [**1**] makes it essential to have some digital version of our identity which is reliable, simple to use and cannot be easily abused online. Consider that online identity fraud already makes tens of thousands of victims every year. Moving online, to an all-digital world makes it both more likely to happen and more dangerous.

Electronic mail has became very common, publishing online one's diary or creating the kind of problems mentioned in the chapter on privacy [**5**] is a popular and pretty easy activity. In spite of this, most citizens and parents haven't realized yet that the Internet isn't just a trendy way to publish boring diaries or read free news and abuse of fair use while it's still possible [**18**]. In other words, almost nobody has already realized how important it is for *all of us* that a viable online identity system is established for both personal and business usage.

Like with any other issue discussed in this book, however, online identity isn't some obscure technical problem only relevant for computer geeks. The fact that, for example, even many Schools and Public Administrations are only going to **increase** their use of computer databases and Internet based services to work for us is enough to make of this another sector where we *all* are computer and Internet users regardless of if, how and how much we personally use these technologies. Is the system ready for this?

The problem isn't easy to frame: what is an online identity? What do you want from yours, that is what should it contain? Just your name or also your Social Security and bank account number, digitized fingerprints [**6**], family status, address, shopping preferences, every country you have visited and so on? When and how do you want and need to merge your online identity with your real, everyday life? Do you need more than one of such identities?

The limits of today's online identity systems

In February 2006 IBM and other companies announced an online identity system called Higgins [**30 - 1**]. Microsoft's has a similar project, called InfoCard, which only works with Microsoft Windows. Symantec unveiled its own "universal ID system" [**30 - 2**], which works for computers, but "can't easily be used with mobile devices", in January 2007.

It is evident that the first problem in this field that the IT industry and our Governments need to overcome is the same for any new technology, especially in the computer world: the lack of interoperability among different systems, that is the lack of worldwide open standards, or the proliferation of incompatible ones. Until this obstacle is overcome, this can only increase the opportunities for computer criminals.

Note that providing a universal identity system connected to the Internet doesn't mean at all, in and by itself, the total, irreversible loss of personal freedom and privacy. Police officers worldwide have been able to share data electronically in real time for decades before the Internet. It all depends from *how* things are done and regulated by law.

There are several, simple basic rules that must be respected (or, more concretely, that everybody should ask his or her political representatives to enforce) for an online identity technology to work as we all need it. Some of these rules are purely technical, that is only define some characteristics of the hardware and software tools used to declare and check one's identity. Others are requirements for new laws.

The first basic rule for a good online identity system is to leave to each single citizen control over what technologies he or she uses, how and when. On the hardware side, devices like RFID tags [**6**], which cannot be activated or deactivated at will by their owners, leaving to *them* the freedom and responsibility to decide *when and to who* to declare their identity, are more a risk than a solution. Imagine carrying an RFID identity card or driver's license that constantly declare to everybody walking by where they can find you tonight or which car in that dark parking lot is yours.

Single sign-on is a term used by software experts to indicate any way to use only one account name and password to access any conceivable online service, from games to information on your pension payments. This is a usability dream on the one hand and a privacy and security nightmare on the other: if that single account/password pair is lost or stolen no service will be accessible and whoever steals the password will know everything there is to know about you. Identity systems must also be affordable for everybody.

Another essential part of every suitable solution must be the *possibility* for individuals to have more than one digital identity profile, each containing different information and having different privacy risks and characteristics. This would be needed also to make the system fully compatible with the laws and social customs of every country. What is essential is still, in any moment, the possibility for any of us of disclosing only what is really necessary, only to those parties which really need to know it in that specific moment.

OpenID: a possible step in the right direction?

There is an open, decentralized identity system available on the Internet which is still in its infancy but looks promising for several reasons. Besides its technical merits, OpenID [**30 - 3**] is very easy to try and use *today.* All one needs to do to establish an OpenID Internet identity is to register, remember and distribute one single Internet Address (which can even be the same as an already existing home page) and properly configure the corresponding web page. After that, it will be necessary to remember and use only *one* password to be automatically recognized on all the websites where a user needs and wants to be identified.

Is this the solution? It's probably too early to tell, but if the Internet must become really helpful in our real lives an open, decentralized and pervasive digital identity system is necessary. It is not possible any more to deny this fact. Whether or not OpenID becomes that system is another matter, but if it's quickly integrated into popular software for website management, it may very well become the de facto standard before anything else. If nothing else, OpenID remains an easy way for everybody to start testing what universal digital identities may look like, and how far along the road they still are.

Chapter 31

Are digital communications safe? Can they be used without hassles?

Nearly instant communication systems like email, Internet Chat, Instant Messaging and so on, at no cost or for a very low flat fee, are the real killer application of the Internet. Today, however, they are still everything but private, safe or hard to forge [**31 - 1**]. Unlike phone calls, email can remain stored in multiple independent locations, even after the message has reached its destination, and presents new opportunities for surveillance. A copy of a message may be stored on the sender's computer, his or her ISP's server, the recipient's ISP's server, and the recipient's computer, as well as back-ups on any of the machines it traveled through. Furthermore, any one of those machines may be equipped with one of the systems for real time text-scanning already discussed in the first chapter on privacy [**4**].

Similar considerations apply to Internet Relay Chat, Instant Messaging and so on. Therefore, now is the right moment to think seriously about the security and privacy of email and all other text-based digital communications. The moment when they will merge with phone text messages and almost everybody will be forced to use them at least once for something important is close.

In particular, it is necessary to start learning how to crypt all digital messages, and about whether it's safe to leave them in the hands of third-party providers without serious guarantees on their privacy policy. Remember again that, even if you don't use these systems, your government and managers already do.

The Big Webmail Brother

Email can be read and received even without installing a dedicated program on your computer [**28**], with the same web browsers which are used to visit normal websites. You go to a certain Internet address, log in with a user name and password, and in the following window you'll be able to read and write email. A big disadvantage of these "webmail" systems is that most of them provide even less privacy and security than traditional email. As harmless and convenient they may seem, they are one of the best places to be spied on, and a proof that you must understand at least the basics of what's happening around us.

Some webmail providers automatically alter all the email you read in a disturbing way. If there is any Internet address in the message (as when your friends send email saying "Hey, check out this article at www.so-and-so.com") if you click on it you don't go to that site right away. You are redirected without noticing to a server in the email provider's site, which immediately redirects you to where you thought you were going in the first place. In other words, rather than going directly to www.so-and-so.com, you are forced to pass through their server first. Sometimes this is a feature of the webmail software which actually protects the users in case they follow a link to malicious websites. In other cases, instead, this is done to register any website for which you demonstrate interest by clicking on its link. This allows the provider to build a profile of your personality that could be used to customize the banners you see, or even be sold to third parties. Note that even if you were forced to agree to their use of personal data to get the account, you must know just how much personal data they have, and that, whatever the law may say, opening people's mail, even automatically, is a gray area to say the least. The Digifreedom website teaches you how to recognize such webmail services.

The plague of spam email and its impact on family Internet fees

One of the reasons why electronic mail is so terribly convenient to use is that it was designed in a more trusting world, with almost no security, privacy or authentication built-in mechanisms that would make its use less easy and flexible. One practical consequence is that, today, up to 80% of all the email on some computer networks is unwanted advertising, called Unsolicited Commercial Email (UCE) or *spam*, for everything from stocks to sexual stimulators. Carrying these billions of messages around the Internet or stopping as many of them as possible before they wastes a huge lot of people time are **really** expensive tasks. Unavoidably, the related costs end up increasing, even if they are never declared explicitly, the monthly Internet connection fees of businesses, schools and families worldwide

Spam exists because it costs almost nothing to *send* many millions of messages. Therefore, even if only one out of a hundred thousand people reads a message and buys whatever it advertises, the whole system is still profitable. Making people pay a fee for each email they send, as happens for traditional letters, would solve nothing: almost always the spammers infect the computers of **other** people with programs which send their messages automatically, counting on the fact that many Internet users are not competent enough yet to secure and monitor their own computers.

A bigger problem is the fact that many Internet access *providers* tolerate spammers operating from their networks or, fearing to lose business, do not immediately block the accounts of customers whose computers have been infected by spam-generating software. They don't really care if this creates problems for their competitors, or for many more Internet users than they have, and drives up the cost of computer based communications, including those from public networks funded with your money.

Public black lists of Internet providers which tolerate spam [**31 - 2**] do exist: if all families, companies and Public Administrations checked these lists every time they needed to buy any Internet service and began to *refuse* to buy anything from any company in those lists or from their resellers, it would be a big step forward in the fight against spam, one which eventually could lower the cost of many Internet connections.

False spam remedies which prevent communication

With the current email system, spam cannot be completely eliminated, but several of the proposed fixes look even worse than the present situation. There is one which is particularly annoying for its victims and damaging for its own *users*, especially because it is a method which often looks the most attractive to inexperienced ones: enter Challenge-Response (C-R) systems.

Their principle is very simple and terribly smart. Apparently, that is. Basically, every time somebody sends an email to you, the C-R software will hold it in a queue and send them an automatic reply (the *"Challenge"*) which asks to confirm that they are human beings with good intentions (rather than some spam-generating program) by visiting a website or sending another email formatted in a special way. Only after this *"Response"* the C-R software forwards the original message. Wonderful, isn't it? In practice, C-R procedures are almost always one of the most effective ways to make sure that you will annoy a lot of people, including friends, potential employers, people on Internet support forums where you asked for technical assistance and, generally, innocent bystanders. Think about it:

- spam is almost always sent with **fake** sender addresses. You will send confirmation messages to people who do not exist or **never** tried to email you anything at all

- if everyone used this method, nobody would ever get any email

- since every spam message generates a C-R challenge email and spam is the great majority of all email traffic, using C-R on a large scale would create much more congestion

- in real life, only people to whom you owe money will go through the hassle of sending extra messages to be sure that you read their original requests. Everybody else will just ignore you and blacklist *your* address as a spammer (hey, you just sent them unsolicited email, didn't you?). Potential employers who invited you by email to arrange an interview, for example, will simply trash your curriculum and call the next candidate if you bother them with such a procedure

In spite of all these shortcomings, some email providers actually have the guts to *sell* C-R services to their customers with the guarantee that *”it will immediately stop 100% of unwanted messages, period”* and without explaining any of the risks. A Brazilian email provider, for example, had the users of its C-R service unknowingly send annoying challenges to so many people that they set up a public invitation to boycott that provider and all its users [**31 - 3**]. As a result, today many of those people are happy not to receive any spam, but don't get any legitimate email either, and they don't know why. Please check carefully before accepting similar offers.

Chapter 32

When does Internet Telephony Make Sense?

VoIP stands for Voice Over IP. Technically speaking, it is a way of carrying real time voice conversations, that is standard phone calls, through the same equipment and lines which transport files and emails, with the same rules, called Internet Protocol (IP), and inside the same kind of data packets.

In practice, VoIP means two very different things. Phone companies, Internet service providers or any corporation can use it to sensibly cut the hardware and management costs of **their** phone calls, that is the ones that they transport on their *internal* networks for themselves or their customers. This kind of usage, that is strictly controlled operations inside completely locked networks, doesn't present serious limitations or risks if done competently. The opposite, that is direct calls between end users, with or without the assistance of a VoIP provider, are an entirely different story.

The main risk of VoIP

Even if the sound quality is not always the same, VoIP conversations are free, or at least much cheaper than traditional phone calls. Most turn-key contracts for residential customers, for example, give the possibility to make and receive calls at the same flat, low rate paid from home even when the customer's "phone" is actually running inside his or her laptop in a Fiji resort. VoIP also has several downsides, however.

If you have ever surfed the Internet, you may have noticed how unbearably slow it can be some times, for example when many people are visiting the same news website in the same moment. Imagine that happening to your phone call. Not just the chat with your aunt, but also your emergency calls. Normally, when somebody dials the emergency number from a standard land line, the call is automatically routed to a special, reserved network which also knows the address of each fixed phone or the cell, that is the local area, from which a cell phone is calling. Without extra machinery, however, the origin of a VoIP call is always the same for all the customers of a VoIP operator: the computer room to which the modems of those customers are connected.

Things could get worst if somebody used the VoIP subscription originally registered for his or her home from a different location, using a laptop computer: if that customer, for example, called the hospital while stopping at a highway motel, the ambulance would still be sent to his or her home, because that is the place to which that VoIP "phone" is associated.

This is not an hypothetical scenario. The amount of emergency calls from VoIP lines is expected to raise to 20 per cent by the end of 2007 [**32 - 1**] in the United States alone, but in September 2004, 911 was still a joke for VoIP customers [**32 - 2**]: when a reporter called 911 one recent evening to report a mugging, he reached a Police Department employee who explicitly told him: *"If you were to fall unconscious, I wouldn't have your address. This isn't good."* Lawsuits over the unavailability of 911 services for VoIP customers have already happened [**32 - 3**].

Other VoIP risks

Right now all is working nicely and without too many attacks only because VoIP is still a very low part of the total amount of phone calls and many critical VoIP calls still take place in very controlled environments.

If not managed properly, however, VoIP may create problems even when you are not in an emergency situation. Some service guarantees, like the maximum disconnection time for network maintenance, may be deeply different from those of traditional services. Some VoIP phone adapters may not be compatible with home alarms systems.

Security and privacy are other causes of concern in an unrestricted VoIP environment. Call interception from anybody, not just law enforcement officials, can be much easier. The same applies to voice spam, that is sending the same recorded message simultaneously to hundreds or thousands of VoIP users: there is definitely a need for authentication and voice encryption in VoIP phone conversations.

Another issue is the fact some software programs can place VoIP calls making any number their user wants appear on the caller ID display of the receiving phone, making some frauds easier. These threats are only beginning to emerge, but over time they're likely to proliferate as soon as more people use it regularly. Last but not least, the quality of service of self-managed, totally free, direct VoIP calls from a personal computer to another is very likely to decrease when the volume of these calls approach the one of traditional conversations. Net Neutrality [**9**] may or may not help in these specific cases.

Working on the solutions

Computer and telecom specialists are already working to fix all these problems, even if some of the solutions aren't ready yet or if some others aren't applicable yet on a large scale or in all countries.

In March 2005, for example, an industry consortium called VoIP Security Alliance (VOIPSA) formed to study and prevent VoIP security problems [**32 - 4**]. The consortium has already produced, just to help the industry deal systematically with these issues, an official classification of the types of security threats in IP telephony, called Security Threat Taxonomy [**32 - 5**].

In July 2005 Phil Zimmermann, an expert cryptographer, started to develop a secure VoIP system [**32 - 6**], called Zfone [**32 - 7**], which should encrypt conversations and let two users verify each other's identity before talking, without relying on software whose source code [**37**] is not open to public scrutiny.

As far as emergency calls are concerned, in May 2005 the United States Federal Communications Commissions (FCC) adopted rules requiring providers of VoIP services that allow a user generally to receive calls from and make calls to the traditional telephone network to supply emergency calling capabilities [**32 - 8**] to their customers as a mandatory feature of the service in the United States by November 2005. These "capabilities" include delivery of all emergency calls to the local emergency call center, together, where possible, with the customers call back number and location information.

In practice, depending on the country, some providers just require that their customers log on to their website to provide their current address. In this way, when you place an emergency call it can be automatically forwarded to the emergency call center closer to where you are, hoping that they are open 24 hours a day, 7 days a week.

Customers, however, would still have to communicate by themselves their new location to their provider whenever they move, even for half a day, if they want the ambulances to be sent where they actually are (obviously assuming that their temporary location **is** covered by the alternative emergency service). Such solutions are also likely to work with only some versions of some operating system, possibly forcing customers to pay a software and hardware upgrade... to save money thanks to the VoIP service.

What to look for in a VoIP offer

The first thing to check when shopping for a VoIP service is the equipment it requires or provides to make or receive VoIP calls. Is it just a software program to install on a computer? If yes, is it compatible with the hardware and software that you already own? If it is an actual phone or any other physical device, does it work also during a black-out? Does it work *only* through an Internet connection, or only when attached to a running computer?

Unless a VoIP service has none of these limits, it is better to also keep a traditional phone line, either fixed or cellular, and make sure that everybody in the household, including children and babysitters, know which phones are connected to a VoIP line and avoid calling emergency services through it. More VoIP information and useful links are available on the Digifreedom website.

The causes of the Digital Dangers

It is now time to summarize the causes and those responsible for the digital mess which **everybody** is living in today. Its main technical and legal reasons are closed file formats and communication protocols on one side, and abuses of copyright and other "intellectual property" regulations on the other. In and by itself, the fact that software and movie corporations try every trick to sell the same stuff many times is nothing new or special: car makers and fashion designers, to name but two very popular industries, have been doing just the same thing for decades. The problem is that software and digital technologies have a much more devastating effect on culture or everybody's civil rights and are still regulated in a way which is both much more incoherent and much more behind the real world than what happens in most other sectors.

The blame for this is distributed, in different measures, amongst practically all the involved parties: overzealous governments and the software and entertainment industry (abuse and suboptimal development of technology), real and fake activists (extremism, fanaticism or opportunism when proposing alternative technological or cultural models), politicians of every party and the general public, which so far, by and large, have been simply happily absent from these discussions. Let's look at these three problems one at a time.

Chapter 33

The need to control the future

"He who controls the present, controls the past. He who controls the past, controls the future." George Orwell, 1984

In the context of this book, "the past" consists of both the corpus of already existing creative works, locked by extending copyright beyond decency, and the huge quantity of digital documents already saved in proprietary or unknown file formats [**40**]. Those who control the end users also control other producers. And those who control production today do it mostly to kill future, potential competitors.

Martin Mystere, the "detective of the impossible", is a very popular comic character in Italy, where the series is produced, and in many other countries. He is both an archaeologist and a computer scientist, always involved in Indiana Jones kinds of adventures. He is also a manic reader, one of those people who would rather starve than stop buying books, magazines and comics.

In a special number issued to celebrate one hundred years of comics, Martin is ported to a parallel dimension, where writing, reading or generally dealing with comics sends you to prison. Only movies usable with expensive, closed access systems, which are only producible by corporations with huge economic resources, are available to consumers.

Eventually, Martin Mystere realizes that the reason of the ban is just that comics (but the same would be true for books or Internet pages) are much cheaper to produce than movies, to the point that almost anybody could communicate through them, not just the government or some corporation. As one Mystere's enemies puts it, comics must remain illegal because "they tell stories which would never make it to television; it would have been too expensive".

What they really want to stop

The analogies between the Martin Mystere story and what is already happening in our lives in this digital era are evident. Very likely, the first things that makes the industry go nuts in all the cases of "intellectual property violation" is not loss of royalties from illegal copying or redistribution of their current works, regardless of what they say.

Today, to see a DVD movie on a computer it's not enough to pay whatever money the producer asks (and let's repeat once more that they have every right to charge for their product whatever they feel is right, and illegal copying is a crime), but you also must configure your very own computer as they want. This is basically like saying that you can be arrested for piracy if you regularly buy the last Disney movie, and then see it on a black and white monitor... Why? Because in this way they can control what all users can do, that is which *other* movies they will be able to see *or make and market* all by themselves, including the next Blair Witch Project or denounce of some abuses of your government. Remember all the problems with documentaries **[15]**? The same happens with software programs.

The real reason why the entertainment and software industries push for DRM **[16]**, Trusted Computing **[17]**, closed file formats and so on it's not just locking all further profits from **past** works, just as much to make sure that there aren't any **future** works done by others.

In fact, DVD illegal copies can be made anyway, but until you can only buy the mutilated DVD players and recorders approved by movie distributors, you are still forced to pay when they start distributing DVD with limited duration or decoding keys (as in ”buy it,but if you want to see it again one year from now, you’ve got to pay for it again”).

Independent creation and distribution of new material with new schemes: this is the real problem and danger for multinationals. Their goal is not just to keep making money on the current artists, is to guarantee that all the **future others**, including our children, can only pass through them. If the whole chain of creating and distributing movies is locked up with technologies only accessible to big corporations with even bigger legal divisions, how would *your* movie, the movie of your civil rights campaign, be seen? Technology is legislation these days.

Chapter 34

Software and copyright fanatism and opportunism

Is it really needed, to make the world a better place, to make sure that only Free as in Freedom software is allowed to exist? Probably not, for the reasons explained in the chapter on software protocols and file formats [**40**]: if only formats and protocols which are Free as in Freedom, that is usable without any limit or discrimination with many different software programs, were used, at least by Public Administrations, all or most the excesses and abuses caused by today's proprietary software technologies would vanish without further effort.

Software embedded in specialized, single purpose devices like cell phones, even if locked with technical or legal means, would not be a really dangerous attack to civil rights and free market. Not as long as it would still be possible, without artificial technical or legal restrictions, to build, sell and use alternative devices which perform the same tasks.

This would not be a defeat for the ideals of Free as in Freedom, or Open Source, software. As one of its advocates put it: "perhaps the moderate position is the most radical of all. That is, if you want to get something done that works for everybody" [**34 - 1**].

In a world where really free *formats and protocols* are the rule, there would be basically no more ways to establish or keep alive a software monopoly in any area where it would hurt the core rights of all citizens. Legally, it would be still possible for companies and individual programmers to sell single licenses of their programs, limiting or forbidding their modification and redistribution: at the same time, the fact that public and private end users could be really free at any moment to migrate to a competing program, because all their data would remain completely usable, would force proprietary software producers to play fair.

This doesn't mean at all that a world where only Free as in Freedom software exist would be a bad thing, quite the contrary actually. It is just that it is probably possible to achieve that worthy goal without limiting any freedom (including the one to produce and use non-free software, when it doesn't really hurt anybody!), and with less effort too. The key is to look at the problem from the point of view of that overwhelming majority of human beings: those who will never write, or **wish** to write, one single line of software.

Unfortunately, such an approach is still against the core mindset of several individual supporters of the Free Software movement. Up until recent times, this wasn't a real issue for the simple reason that software was visible and relevant in everyday life only for a few specialists. Continuing today to look at the Digital Dangers only as a software hard core enthusiast, instead, may keep alive a split between well-intentioned activists and the general public which becomes more dangerous every year.

A similar danger exists with anti-copyright extremism. Limiting the extension and reach of copyright would eliminate all the current abuses [**2**] without preventing creation of countless creative works, including those in the non-fiction field.

When ideals are an excuse

Almost all activists of the Free Software and Free Culture movements are very coherent people who are right on all the main points and honestly believe and practice without exception everything they preach. Acknowledging this must not lead, however, to ignoring or dismissing a not so pleasant reality. Far too many people have only vaguely heard some random bits of these ideals and proposals somewhere online, and mindlessly repeat them, to themselves and to others, as an excuse to just take what they need without compensating in any way those who created it. Such a "philosophy" was summed up very well in an online forum as:

- Information, knowledge and culture want to be free!
- ...You mean that **you** want information for free, don't you?

and it is very convenient, since it gives (apparently, that is) a noble justification to what is nothing more than lack of critical and independent thought, as well as of understanding of what is really happening. This attitude is particularly frequent among teenagers, who by and large:

1. are under very heavy pressure to consume **without** thinking
2. haven't spent enough time yet to really think the whole issue over
3. do not have enough self-discipline or the right cultural preparation and are encouraged to stay that way (see point 1)
4. almost never have parents or teachers who *are* informed enough to help them

The purpose of this book is to solve the last problem, but the general issues remain: without a more balanced Free Software and Free Culture activism, or without a coherent and informed education, short sighted extremism and selfish opportunism will continue to favor the Digital Dangers, instead of fighting them.

Chapter 35

Ignorance and apathy versus equal opportunities

Everything in this book demonstrates one thing: ignoring how digital technologies work and are regulated, or how ubiquitous they already are, can seriously complicate (or worse) one's life. What the Digital Dangers really destroy are equal opportunities: in every field of activity, not just software design or composing music. Everybody can write a Nobel Prize novel or scientific paper with a Bic pen: the result will be just the same, and be just as useful to society, than if a gold-plated fountain pen had been used. Things change completely when those same works can only be written or read with one thousand dollars worth of hardware and software. This is what making OpenDocument [**41**] mandatory in Schools and Public administrations, for example, is all about: not to eliminate profit and initiative, but to eliminate all artificial barriers to access to profit and initiative.

The only reasons why this has not happened yet are the speed with which digital technologies have invaded everyday life in the last ten or fifteen years, and the level of real knowledge on these subjects, which on average is still terribly insufficient.

If issues that everybody understands instinctively without being a specialist, like keeping bacteria out of drinkable water or food, were managed with the same fairness and rationality as software and distribution of creative works, there would have been revolutions and street fights worldwide several years ago.

This is not an insult to ordinary people, just an objective assessment of the current status of things. It doesn't matter that many more people than ten years ago now have a computer at home or in the office, have been on the Internet a few times or even every day without (apparently) hurting or embarrassing themselves. The truth is that anything remotely digital [**1**] or related to software is still seen as black magic by most of us, and most computer users still push buttons without really understanding what is happening.

This is OK, we don't need to became all programmers [**43**]. Even among software professionals or those who have graduated in any field in the best Universities, the lack of perspective about this discipline is still much bigger than in many other fields of human activity. One of the best proofs of this fact are the many software professionals who still see no problem in the file formats field [**40**] but spend all their time and energy worrying *only* about how the source code [**37**] of a program is developed or shared: that **is** indeed a huge problem, but not the main one in many cases, and in many others becomes relevant only because no open formats and computer protocols are enforced.

Trouble is, we can't afford this confusion anymore, because software and digital services or creative works are already so persuasive that they greatly influence the quality of our lives and of that of our children.

Luckily, another thing that should be obvious, or will be obvious by the end of this book, is that one does **not** need to become a technical expert, or spend a lot of time, to have these problems solved for good. Many of the solutions are based on requiring the right laws and voting with one's wallet. The only effort lies in understanding what to ask for and why. In other words, if this situation continues till it's too late to go back, today's children will only have their parents and teachers to blame for it.

Chapter 36

How to tell if all the programs and games inside a computer are legally usable

Don't listen to popular wisdom and urban legends: in almost all countries of the world, installing on your computer or sharing music, games, movies or software programs with others is legal **only if explicitly allowed by their user license**. In all other cases it is a crime that has **already** brought lawsuits to unaware parents [**13**].

Finding out if all the content of a computer is legal is very easy. Software, for example, is not sold nor given away, regardless of the appearances. Each software program is distributed with some conditions for using it legally, called a *license*. Some licenses are written to forbid modifications and redistribution of the program, in order to maximize the profits of the company which developed it. Others, like the General Public License (GPL) of the Free Software Foundation, are specifically designed to make sure that all the users of a program can study, modify or improve it and redistribute or use the improved source code [**37**] without restrictions.

In other cases the software is literally given away, that is abandoned for everybody to take, and maybe resell, as he or she pleases, without any conditions. When this happens, however, it is still thanks to an explicit decision and declaration from the software author.

Incidentally, none of these licenses guarantee that there will not be loss of data due to defects in the software or that, in such cases, there will be a refund. Software is so complex and it is used in so many different ways that, in almost all cases, it wouldn't be possible to offer such guarantees: still it is important to know that one of the most common reasons for buying proprietary software (*"we know who to sue to have refunds if this doesn't work!"*) has basically no basis in reality.

An end user must simply look at the kind of license and distribution model. For example, any program developed and distributed as Free or Open Source Software is surely fine to use, copy, install, modify and redistribute under the same conditions. The important thing here is to **not** trust common wisdom or whoever made you use some software on this.

Many people, for example, still believe in good faith that they are safe from any legal trouble if they install without paying, "just for personal, non-profit use at home", any software which is sold in the stores. This is almost never the case: more exactly, this is **never** the case unless it is explicitly written, on the CD-ROM or in the installation screen, that such an use is allowed. Another common case where people and families end up violating the law against their will, or without even realizing it, is when some software is installed on the home computer because it is the only one with which it is possible to complete some school project.

In these particular cases the assumption, or sometimes the hope, is simple: if a teacher put a student in the need to install a program on his or her personal computer, without checking if the student can afford to buy that software and actually buys it, everything is surely OK. In other words, parents (must) assume that either the teacher knows it is certainly legal for the students to not buy a software license or that, if a crime is being committed, only the teacher will be held responsible. Nothing could be further from the truth. First of all, if a software license normally requires the payment of a fee, it is **never** legal to install and use it at home unless:

- there is an official student edition or similar offer at reduced price, or:
- the documentation or installation procedure, again, *explicitly* allow personal use for study

In the second place, installing software without even pondering for a moment if it is legal to do it, not knowing in the first place that it *may* be illegal sometimes to do so, or lacking a real understanding of these issues are all phenomena still too common among many *teachers* to assume that they were able to do this kind of research for their students and actually did so. This should not be taken in any way as an insult to the millions of teachers worldwide who work hard to educate their pupils in the best possible way: it is just an acknowledgment that these problems are still so new, and the interest in the status quo so powerful, that so far there has been very little time or opportunity to inform and train teachers in the proper way.

Therefore, unless you are already absolutely sure that it is OK to install and use some software, always ask its author, distributor or the teacher who makes you install it, if it **is** indeed OK to install and use the software as you intend to do. The same rules apply to computer games, music, movies and so on. Remember also that, even if it is (still) very easy to foul proprietary software licenses and installation procedures, you are shooting yourself in the foot in some other way tomorrow, by giving the industry valid excuses to make computers impossible to use as it is today [**17**].

Chapter 37

What in the world is this ”source code” anyway?

The source code of a software program is the complete description, in a (theoretically) human readable programming language, of what that program must do. For 95% of human beings, this sounds like one of the most boring and useless things to know or look at. However, even if almost nobody has to look at any source code, the way it is managed is still crucial for our lives and civil rights, not to mention, sometimes, national security [**24**].

Source versus machine code

Internally, computers do not need source code, nor would they be able to understand it. The only instructions that any microprocessor, the central electronic circuit of every computer, can directly understand are *machine codes.* These are special sequences of bits (1’s and 0’s), each of which corresponds to one specific operation which the processor is able to execute at very high speed: things like sum, multiply, copy data from one location to another and so on. Any software program, no matter how complex it is, is just a sequence of instructions in machine code.

It is possible to write programs directly in machine code, but it is a very boring, complicated and error prone activity. Since only very elementary instructions are available, it is necessary to write a lot of them for even the simplest task and, even for a competent programmer, the resulting code is very hard to read and figure out, especially when it is necessary to update or modify programs written by somebody else. For all these reasons, machine code is written by hand only in special situations where it is absolutely necessary to maximize the performances of the computer by giving to it the smallest possible number of low level instructions.

How source code is used

Today it is possible to describe the behavior of a software program in a wide variety of computer languages at a much higher level than would be possible with machine code. These descriptions, that is the *source code* of the actual programs, are then translated into machine code by specialized programs called *compilers*. The process is semiautomatic, since the compiler needs specific instructions to perform the conversion in the optimal way.

The development of compilers and the related possibility of writing and modifying only source code in high level computer languages has been a huge step forward for software engineering and society as a whole.

Every software language has high level operators which allow one to express the basic steps of any generic procedure: some of these operators mean things like ”if this is true, do X, otherwise do Y” or ”write these data to a file named Z”, others can describe with one or two keywords very long sequence of repetitive instructions or very complex mathematical operations.

Thanks to all these features, writing programs in a high level software language takes much, much less time than doing the same thing in machine code. The same applies to correcting errors, adding new capabilities to a program or merging two programs into a new one. Machine code is also very dependent on the physical structure of the processor which executes it: as a general rule, the machine code written for one processor cannot run without heavy changes or a complete rewriting, on any different processor model.

This doesn't happen with source code, because it is written at a higher abstraction level. Besides productivity at the initial stage, the first time a program is created, this gives another huge practical advantage: *portability*, that is the capability of generating different versions of machine code, each optimized for one specific processor or operating system [**3**]. In order to create a different version, the programmer only needs to give different instructions to the compiler: there is no need to rewrite the whole program from scratch.

Why it is necessary to know what source code is

Besides the huge improvements to design and maintenance, source code is also essential to figure out how a program really works. In other words, studying the source code of real, widely used software and, if possible, improving it, is by far also the best possible way to *learn* programming well enough to make a living (or anything else really meaningful) out of it.

Source code is also all that is needed to generate a working copy of a software program perfectly equal to the official one distributed by the original author. For this reason, controlling by law how source code can be distributed, or if, how and by who it can be modified, is a very powerful economic weapon for everybody who wanted to either stimulate or prevent competition in the software industry. Last but not least, access to source code, to check without intermediaries the presence of security problems, is vital for every software program used by military equipment or when, for example, the software shall be used to protect state secrets.

Chapter 38

What is "Free Software"? Is it legal?

You may have heard of something called "Free as in Freedom Software" which is causing a lot of noise among ICT professionals. Why all this fuss on software given away? Can it be any good?

Free Software is a movement officially born in the early eighties in the USA. The word "Free" in "Free Software" is usually explained as "Free as in free speech, not as in free beer". In general terms, the definition applies to any software on which the author has not forbidden changes or redistribution by default. In other words, the author may still make a living by directly selling or supporting the software, but each copy can be modified and/or installed many times by the end users, and redistributed too, under the same conditions, without paying any license fee. The reasons include mutual support, efficient development of better software and facilitating the sharing of knowledge.

This model doesn't work just for toy programs. Many of the extremely stable tools and protocols that keep banks, military bases and the whole Internet running today have been created in this way, and are still available at no charge. These tools were originally developed by people and institutions who made a living in some other way, and who just needed to exchange data or knowledge amongst themselves.

The fact that nobody ever needed to sell these programs for a living is exactly the reason why they are so stable and powerful. They were never loaded with useless frills just to impress Wall Street, and nobody ever needed to put together too many bogus versions, just to release something, anything, ahead of competitors. This is also the same reason why this kind of software, and the communities around it, often appear less user friendly and more limited to specialists.

Is it legal to give this stuff away, or to take it?

This is not a stupid question. Even such an apparently obvious freedom is far from being granted these days. The answer is that, within the limits of copyright, patent and trademark laws, what matters is the will of the software author, which is expressed in the license [**36**] which comes with the software itself. If a software program is licensed under the terms of the General Public License of the Free Software Foundation or another license with the same or similar spirit, taking, modifying and redistributing it is not only allowed, but encouraged.

Is it bad for my country, or the economy?

The Internet and many, many fundamental concepts of computing have been around, always freely available, for much longer than advertising would like you to know. It is not only possible, but fully legal and quite often better-performing and profitable to use digital technologies which the mainstream media still often dismiss as toys, useless eccentricities or almost illegal tools.

A common argument against more open technologies is that they stop innovation, because in the future they may make it much harder to become the richest person in the world by only working in the software field. This would destroy any incentive to innovate and punish initiative: *"What if some student here were a potential software mogul waiting to rightly become a millionaire? Would we* *be right in stealing his or her opportunities, to say that everybody could copy his or her software?"*

This is the wrong way to look at the problem. First of all, there is no real need to force anybody to give away his or her work. Anybody can license his own creative work in any way he or she sees fit, as long as the relevant laws are respected. In the second place, this attitude is exactly what is closing the road ahead to many excellent programmers. It is exactly because the first comers were able to lock all the gates behind them that it has been necessary to start antitrust investigations, on both sides of the Atlantic.

Another false belief is that the Free Software philosophy, or at least its followers, are in some way"communist", i.e that adopting such a philosophy is some anti-historical attack on merit, free markets and private propriety. The truth is that really open communication technologies are an idea, first at the ethical and then at the purely practical and economic level, just too good to be ignored or boycotted. They are not again merit, initiative or profit, only against monopolies.

What is also true is that one "limit" of these technologies is that they demand more education and conscious thinking, but this is something which is much less of a problem than it looks as we will see in another chapter [**43**].

Is Free Software only relevant for programmers?

Not at all. Demanding a wider adoption of Free Software, starting with Schools and Public Administrations, can be one of the easiest and most effective ways to fight Digital Dangers. Even if one will never use it personally, making sure that everything that can be done with a computer can be done using exclusively Free Software if the end user so wishes is essential to stop many of today's excesses. Having a Free Software version of any program, means having an already working set of source code for any problem, which solves it and can be legally modified or redistributed without asking permission or paying high fees.

Practically speaking, what becomes possible for all citizens in such a case is having *local* programmers competing in making custom versions of any program with more functions and/or an interface in any native language: in other words, local jobs and a better service.

The unreplaceable role of source code availability in education and national security, made possible by Free Software licenses, has been already explained in the corresponding chapter [**37**]. Being highly customizable, Free Software is also an excellent way to extend the life of computers, thus reducing the pollution caused by software [**19**].

Free Software can also be an excellent choice for senior citizens, because it is perfectly legal for a specialist to modify it to make it run with a very simple interface on very inexpensive computers. Such computers are just what would allow to many people to really control, for the first time, how their Government is spending their money [**26**].

Another reason why Free Software could be the best way to introduce senior citizens or anybody else to computers and the Internet is the fact that it also makes remote administration easy and, if there is a cheap or flat rate Internet connection available, much more affordable. Something goes wrong? Unless you physically break something, no problem! Just call your grandchildren or a specialized technician with a service contract and they'll fix it from their home or office!

Chapter 39

Must all software, be free, or all proprietary?

One of the main themes of this book is that there is a strict relationship between software and your civil rights. As we already said, "technology is legislation". We have already seen that we all pay a much higher price than we would ever have suspected [**3**] for the software used **around** us.

The answer to the title of this chapter, however, also depends on the kind of software and hardware involved. Keeping a word processor, or at least its file format, Free as in Freedom is a must. The same may be said for almost all the formats and protocols [**40**] used to communicate through general purpose computers. Keeping closed the software inside a special, single-purpose device, like a cell phone, *may* have less harmful consequences for society instead. In some cases, as with wireless devices, it may be **better** not to disclose, or keep it illegal to modify the software controlling them. Hacking the software inside a radio transmitter to increase its transmitting power, so that it can reach your neighbor's computer to play together, may be harmful for the health of other people or interfere with other radio devices that they own.

Should commercial software die?

Free Software doesn't at all mean promoting software piracy and/or imposing any restriction on market economy. Whoever creates software (or any other kind of creative work, for that matter: books, music, video..) is fully entitled to dictate any price and/or restriction on its use within the bounds allowed by law. Not paying the required price and/or violating the license terms is illegal, and must be prosecuted.

This said, Free Software is an excellent thing for all the reasons listed in the previous chapter. Does this mean that the current model of commercial software, with license fees for every copy of the program is wrong and should be abandoned? Does this mean say goodbye the market economy, at least in software, or that software "piracy" should be institutionalized?

Many people, starting from the members of the Free Software Foundation [**39 - 1**], believe that all software and digital technologies should be Free (as in Freedom of speech, regardless of their price). That could certainly be a good thing, which would also change the nature and geographical distribution of many software related jobs, not necessarily their number.

At the same time, the availability and widespread usage of really open technologies is just a decisive, irreplaceable instrument for achieving much more important goals. As the many examples in this book prove, a world where digital technologies are really open and correctly regulated is a world with more freedom and personal or business opportunities for everybody, not just programmers.

Computers and the Internet are becoming essential to practice freedom of speech: asking for open and affordable communications technologies and fair laws means asking for a world where everybody who can speak online can do so, at the smallest possible cost, and all other human beings can freely choose, at the same cost, to listen at the same time.

In this context, a free software market is needed and good, but only when it **is** actually free and open, i.e. not spoiled by any monopoly. What matters is to make competition, profit and innovation possible without forcing anybody to use any specific program, even if it's Free Software, that is, again, to use non-proprietary formats and protocols. In such an environment, Free and proprietary software could coexist, to each other's advantage and without real harm to society.

Which Free Software is the most needed?

Software-wise, the most practical and freedom-loving way to a better world is to make sure that everybody should have the freedom to use whatever software he or she wants, and to ignore what software others are using. Trying to force people to use **any** kind of software is wrong. Besides, in the real world, what really restricts people's freedom are file formats. Breaking such chains for good might not even require any action or (self) training effort from most end users, at least in Public Administrations, which is where a lot of our money is spent. As far as office documents are concerned, for example, it could be enough to just add some component capable of supporting OpenDocument [**41**] to their office software, if it is still missing, and configure the program so that, by default, they only save documents in that format.

This would be great for people (no need to buy a new computer to read a document issued by **their** Public Administration) and for all computer users, because in this way they arrive, without effort, at the point where they can really freely decide whether or not to keep paying for the next version (and nobody suffers from their decision).

Such software components already exist [**39 - 2**], even if they are still being polished. What remains is to make it mandatory that such components are used, that is to demand that only proper file formats like OpenDocument are used when communicating with Public Administrations, or for archiving all public documents.

Chapter 40

What are protocols and formats anyways?

We have already mentioned protocols and file formats several times, saying how important it is that they are open. Now let's look at them a bit more in detail, in order to understand what these things are and how, and above all why, they can be made open (or closed, for that matter).

What are computer and communication protocols?

A protocol is a set of rules defining which messages two entities can exchange, to accomplish a task. The two entities can be either humans or computers. In the human case, for example, all the things to do or not do on the first (or on the third) date constitute a protocol, even if it is not an immutable one.

To understand even better just how important protocols are, try to compare operating systems and computers to people's brains, and protocols or file formats to languages. Imagine that each human being was skillful enough to build his or her very own, one-of-a-kind computer, running unique software.

As long as all these computers were still using the same communication protocol, you could still have an Internet, just as millions of human beings with largely different brains can still communicate about many things without any ambiguity, as long as they use the same language and, of course, don't lie.

Protocols also define how the messages are formatted, i.e. of which and how many symbols they can be composed, and how to handle errors or interruptions in the communication.

What are file formats?

Any document stored as a sequence of digital bits [**1**] inside a computer is a file. A file format is the set of rules that specify which bits mean what depending on their position and order within the file itself. A certain sequence of bits right at the beginning of the file, for example may mean "this is a text document created (and editable) only with the program called XYZ 2007". Theoretically, the same sequence of bits later on may mean an altogether different thing, like the letter W, or "Underline the following word".

The critical role of standards

Computer formats and communication protocols have real value only when they are formally recognized as official *standards.* As far as we are concerned, a standard is any set of rules which describe in full detail how to accomplish some generic task, which has been accepted by the computers, individuals or companies usually performing that task. A standard can be proprietary or non proprietary, open or closed.

In this context, closed means that *not everybody is allowed to know what the rules are*, or is allowed to use the standard altogether. You might have to pay a fee, commit to respecting some terms of use, or be simply told that you have no business looking into the standard. Non-proprietary means that the rules do not belong to any single individual or company, but to some (generally non-profit, more or less open) community which has been acknowledged as competent and the ultimate court whenever the standard itself is concerned. A non-proprietary standard is something that only the whole community maintaining it can change. A proprietary standard belongs to one (maybe for-profit) company. Even if it is entirely published, that company can change it at will, whenever they feel like it, and without being forced in any way to inform all others of which changes where made. End users don't notice this fact because they continue to do the same things in the same ways with their computers. Of course, this is true only as long as the company which owns the proprietary standard continues to release its software and as long as the end users can afford it.

For proprietary software producers, closed standards for file formats are an excellent way to force their customers to keep buying only their products. Once a personal diary, a contract or a business report have been saved inside a computer in a format which can only be read by one software program, never mind copyright! That document belongs to the developer or company who developed that program. There is no way to retrieve it, unless one is a very competent programmer with a lot of spare time, if the original program itself cannot be used anymore because it became too expensive or for any other reason.

Only through closed standards software producers can ask and justify higher prices at every release [**3**]: their position is that they only have incentive to innovate (for the common good, of course) if they know that they can get such prices for new versions forced on end users every few years. If any bright idea should pass through the slow procedures of some committee, they say, and eventually be made public so everybody can make a profit out of it, it would be the death of innovation. The truth, instead, is that society can progress **only** if most computer file formats remain stable, completely open and there are no unnecessary duplicates. Humankind went in just a few centuries from runes on stone to wireless instant messaging, passing through printing presses, typewriters and fax machines. This happened *exactly* because the alphabets remained almost unchanged in that whole period, preserving knowledge: if every generation had had to stop to rewrite every written document in another alphabet, nobody would have get anything done.

What should be freely usable?

Most file formats and protocols, of course, or at least the ones necessary in education or official government procedures and documents. The real stranglehold of software programs is not the user interface or finding any software already bundled in a new computer, but the file formats, as long as they too are designed and developed mainly with marketing criteria.

Think of software as pens, and file formats as alphabets. Alphabets are as valuable and essential as the very air we breathe. The fact that they are free of charge doesn't make them worthless. Are the alphabets with which the Declaration of Independence, the Odyssey and the Holy Writings of any religions written worthless?

Would you accept paying for the private or business use of an alphabet, or for each hour you use a pen? Try to imagine any manager saying "OK, we have one hundred employees who will be taking notes by hand simultaneously, so we must put in budget funds for one hundred alphabet licenses. Hey, wait, we'll be writing capital letters too, let's buy the professional edition".

It is exactly the usability of all alphabets at no cost, without restrictions, that makes a lot of good things possible.

If you break the monopoly on pens, but leave the alphabet monopoly intact, it's worthless. Real freedom, as far as computers are concerned, is not "let's all use or develop software only in **one** way"; it is the freedom to ignore *which* software programs your neighbors and partners are using, or to change software without losing your data, and still be able to work together. This is the freedom from which all the other software related freedoms could come from. What is needed to practice it is non-proprietary file formats and communication protocols.

Switching to such formats and protocols is much more important (with some essential exceptions discussed in another chapter [**44**]) than non-proprietary software. The file format, or at least the nature of its specification, is very often the only issue that every citizen should care about: if a computer file format is free as in speech, without restrictions on its usage and fully described, the end user is free to change software at any moment, for any reason (price, support, look and feel of the user interface, memory requirements...), because his or her files will remain his or hers: fully usable with any other software, without being forced to upgrade every year or to waste time converting documents and configuration data from one "Free as in Freedom" format to another.

Which File Formats Are Acceptable And Safe to Use?

Once you understand what a file format is and why open ones are essential, the hardest part is done. You just have to choose once which formats are better for your needs and those of your government, and stick to them, until your needs change or new formats, technically better but equally open and Free as in Freedom, become usable.

When it comes to word processing, presentations and spreadsheets, the choice is easy: just go for the international OpenDocument [41] standard, which can already be used on all the most common operating systems.

Remember that another popular choice for this kind of documents the Portable Document Format (PDF) is good enough only if the document must not be edited anymore and/or you haven't any other format, or if you don't care at all about all the *internal* information in the document (like, for example, spreadsheets formulas), but only want to preserve what the document looks like when printed. The same limits exist also in the PDF flavor specifically created for long term archival, PDF/A.

Besides office documents, there are other important file formats that should be preferred in other fields: digital pictures and other images, email, digital calendars and so on. They are all explained on the Digifreedom.net website.

Chapter 41

What Is OpenDocument?

In the last decades, file formats have been used by several software companies to avoid free market competition, making it harder for customers to switch to newer and better products, or to place restrictions on how people use programs or the information produced with them. This is a well known fact which has happened in many fields, from engineering to movies [**41 - 1**].

Today this problem is particularly evident in the office automation world. What makes it possible for only one office suite to remain the one which is installed, no matter how expensive it is, or how heavy its hardware requirements are, in almost all the Schools or public and corporate offices of the world is not its quality. It is the fact that billions of public and corporate files are *already* locked up in a format that only *that* piece of software can decode, modify and display without any error or limit. The consequences on the world economy, in and out the software sector, are remarkable. No matter where you live, to make business or, in general, exchange complex documents with almost all Public Administrations or companies, you have to use one specific brand of software.

To figure out how ridiculous this is, try to imagine if there were the same requirement on paper documents. How would you react if your government told you *"We accept tax forms, driver license applications, tender proposals and any other similar document only if they are filled in and signed with THIS brand of ball-point pen,* *even if it is the most expensive one"*? Still this is exactly what is happening today, and it doesn't stop at office software.

Since that office suite is the only one which, regardless of merit or price, can or *must* be kept in so many computers for the reasons above, the same happens to the operating systems on which it runs and, by reflex, on many other software programs which run well, or run only, in the same environment. These monopolies are then propagated in the homes: it's just natural (or unavoidable) to use the same software that one knows from the office or that, for the same reason, is preloaded (that is charged, even if you didn't want it) on almost all new computers.

To sum up, this de facto monopoly on office documents is one of the main reasons why several of the Digital Dangers described in this book are still such a big deal for every parent and taxpayer. Today, however, this is also one of the fields where, at least for the future, it is easier to switch to a definitive solution.

Enter OpenDocument

Today there is a file format which is made to order for all usual office documents (texts, presentations and spreadsheets), doesn't force its private and public users to use only one office suite and doesn't have, in and by itself, any black box that could make it useless for storing important information in digital format. This format, called OpenDocument [**41 - 2**] has been developed by a nonprofit consortium and formally ratified in May 2006 under the name "ISO 26300" [**41 - 3**] by the International Organization for Standardization (ISO). ISO is the same organization which defines, in a non partisan manner, a lots of other rules without which doing business or having fun would be either impossible or at least much more difficult, expensive or risky than it is today. The formats of CD-roms (ISO 9660), paper sheets (ISO 216 [**41 - 4**]) or alpine skis mountings (ISO 10045), as well as the admissible burning behavior of bedding items (ISO 12952-1) or the safety requirements of powered toothbrushes (ISO 20127) are all examples of ISO standards that already make our own lives easier and safer.

Being an ISO standard is not the solution to all problems: it is still possible to have ISO standards which are technically flawed or duplicate other standards just as an attempt to keep existing monopolies alive. The ISO label, however, remains a very, very strong guarantee that something has been thought through, structured and at least documented in a complete, impartial and professional way.

This is why OpenDocument is so important in fighting Digital Dangers: its many purely technical merits and its ISO standard status guarantee that it is sufficiently featured and well documented to be really usable with many different software programs, thus protecting consumers (and government) choice. Note that, just for this reason, being an ISO standard is a mandatory requirement for many technologies to be even *evaluated* for government adoption.

Back to office documents, other standards *may* be better than OpenDocument as patches to limit the damage which has already been done, that is to convert *already existing* files to formats which are more likely to remain readable by future generations. Only OpenDocument, however, due to its future-proof, "open by design" nature and the fact that it was not created by only one private company to document and replicate the behavior of its own software, is an acceptable choice for the near and long term future. If OpenDocument became the only accepted format for exchange and archival of new documents in all Public Administrations, the chain effects would be so big and beneficial that many people may just stop worrying about many Digital Dangers inherent in the current situation.

OpenDocument Traps

Sooner or later, every producer of office software will be forced to support OpenDocument. By design, however, this standard doesn't limit or restrict every possible detail. For example, it doesn't specifies a single format for images embedded in documents. The practical consequence is that nothing prevents a program from creating files which fully respect the OpenDocument ISO 26300 standard, but are just containers of images and other components which are in proprietary or unknown formats, using this "100% OpenDocument compatibility" to keep winning governments contracts worldwide, while still locking out everybody else.

This is a very concrete risk that could nullify all the potential benefits of OpenDocument, but it is not a technical issue. A technical specification cannot and should not contain, allow or forbid everything under the sun. This is a separate lawmaking and "trademark" issue. The complete solution to regain public ownership of public documents is to to create something like an OpenFile trademark which is applicable only to OpenDocument files in which no component is usable with only *some* programs, and then require laws that make files with that "trademark" the only acceptable ones for exchange and archival of public documents.

Chapter 42

How to protect privacy, or at least limit the damage

The first and most important thing to do to solve the privacy problems described at the beginning of this book is to not believe that you are immune; the second is to acknowledge the problem without getting hysterical. The third is to implement, or ask that governments implement, the social, technical and legislative solutions described in the rest of this chapter. Many of the right things to do are based on common sense, more than deep technical knowledge, and most of them are valid and do-able even for people who don't own a computer.

Social and cultural steps: there is only one you, and now everybody can see it

As F. Stutzman, a researcher at the University of North Carolina puts it, *"you don't go walking round the mall telling people whether you are straight or gay"*. Almost everybody instead, especially youngsters, still behaves online as we've been used to doing for millennia: on the assumption, that is, that behavior and language at home, in the office or at the pub *can* be different and remain separate. In a sense, we all rely greatly on this segregation of different contexts to function. Online, however, keeping the several sides of our personalities and lives separate requires a much more conscious effort and skills other than those most have used so far, or are technically capable of using.

"Jean" may insult or ridiculize "Nick" in some online chat just for the fun of it and, on the same day, answer a job offer for English Literature teachers published online by Mr Jones, the principal of the Community College of her native town. But there is no guarantee that Mr Jones (or any of his students) is not "Nick", or that he won't easily recognize "Jean" just because insults and job applications took place in two different computer windows, or under two different names. According to a July 2006 survey, 27% of USA employers already check the profile of all their job candidates online [**42 - 1**]. This happens in the same world where many people who use the Internet still mix everything from their CV to their musical and sexual preferences on the same home page, or manage the same data in such a way that they all turn up together anyway in one single, public Internet search, no matter who performs that search.

The Internet gives us all the power to tell the world about a boyfriend who cheated on us, even if it was partially *our* fault and even though our complaint stays online to demonstrate that *we* acted without real consideration. It is essential to keep this in mind and teach it to minors, to protect their privacy and future. In this sense, the Internet may even end up having a beneficial effect on manners and social responsibility.

Of course, there is also potential for dangers and abuse in using computers and the Internet: while indiscriminate Internet censorship is bad, saying to a child "OK, put your pictures, feelings and address on the net for everybody's pleasure" cannot be done without control.

The solution is easy to explain: parents must watch over their children anyway, whatever they do, as well as talk and listen to them. If computers are involved, asking that the whole Internet be censored wouldn't solve anything (even if this were possible). The right thing to do is to make sure that the computers at home and school practice some kind of access control that blocks what YOU consider to be inappropriate [**29**].

Technical steps

The most common way to have your credit card number stolen is still through old fashioned shoplifting, copying it when you hand it over at a store and so on, even if you never use a computer. It is true that Internet purchases give thieves many more ways to abuse an *already* stolen credit card number, or that using your credit card online *feels* much less secure than handing it over to a waiter who then disappears into another room for a few minutes. It is essential, however, to be paranoid only when really necessary. Don't let your credit card disappear from your sight and check its balance as often as possible. In this sense, technology, that is the possibility to check the balance online, any day and time of the day, is a godsend.

If you own a computer, take the steps described on the Digifreedom website to protect your privacy. They go from learning how to encrypt and digitally sign all your personal and work email to using a professional and privacy conscious email provider. Also remember to always take the time to carefully check the privacy and data retention policies of all the online services you use.

Political steps

There is no longer any doubt that every family has to ask for better laws to protect its privacy from the risks and accidents described earlier in the book. In this context, it is important to never forget that the most important thing is not to refuse technology tout-court but put, whenever it's necessary, clear and fair limits on how it can be used [**42 - 2**].

Chapter 43

Must We All Become Computer Programmers?

Relax: nobody is going to ask you this, nor should they. It is foolish to assume, as many Free Software activists more or less unconsciously do, that you should directly contribute in some way to develop the software which you happen to use. The idea of contributing to the community is wonderful, but restricting its definition of community to all and only the *contributing* users of some software program would be ridiculous or elitist.

Users or programmers?

What do we want our children, students or country to become? Software end users or software developers? It would be useless, counterproductive and terribly boring if everybody became a programmer, but is it still possible to remain ignorant users? Unfortunately, the easy answer, that is "of course, since I just want to ignore what software is" is no longer viable today, especially for responsible parents and teachers. In their shoes, it would be like asking: "Do I want (can I afford/should I bother) to teach my children or students to write, or can I just tell them to hire somebody to do it whenever they need it?".

In the workplace, continuing to completely ignore what Digital Dangers are would be as safe as accepting an invitation from some consultants to focus on the core business without bothering anymore to read, write or multiply by ten, since they can do it for a fee.

The Internet, word processing and software in general are, de facto, being added to and sometimes replacing reading and writing as the basic cultural and survival tools in modern society; there is no choice: we, or at least our children, all have to learn to use the basic tools by ourselves, very much as we would not accept paying somebody else just to read us the grocery list, and understand what these tools actually are.

Technology by itself will never make our life better, but it has also become something whose control is not to be delegated, lest we lose our freedom, or the possibility of gaining or preserving it.

So, while it is not necessary to all become programmers, it is essential to be able to recognize incompetent reporting in the news and, generally, take informed decisions where technology is concerned. Even if the only thing to decide is which political candidate is best suited to fighting Digital Dangers on your behalf. There is no need to subscribe to all the software magazines one can find to do this: reading and using this book and the associated online guides, from the one listing bad technology journalism to the database of Digitally Free Schools [**47**], is an excellent start!

Chapter 44

What Can I Do As A Citizen?

As Spiderman would put it, "with great power comes great responsibility". This is an age where there is the possibility of improving your life and everybody else's as well, through the better use of computers and digital technologies. In order for this to actually happen, however, it is necessary to act: sometimes with your wallet, sometimes behaving smartly and sometimes demanding laws that protect and stimulate initiative and talent but, above all, fair competition and equal opportunities with access and use of digital technologies.

The Pension Funds weapon

In general, each individual should have as much control (or information at least) on his retirement funds as possible. Now, as even Jeremy Rifkin pointed out in his book "The end of work", pension funds depend on the stocks of the very companies that sometimes put people's pensions at stake. The fact that a pension fund itself can create trouble for such companies threatening to sell or not buy the corresponding shares, should not be undervalued. So, whenever it's possible, it can help to check if and how much your pension portfolio relies on commercial companies which perpetuate Digital Dangers. Teachers and parents have twice the reasons to do this, since their actions, or lack thereof, will affect and limit their students or children much more than themselves, regardless of what those children and students will do with their life tomorrow.

Vote for a reform (not abolition) of copyright

Copyright is heavily abused nowadays. There is no doubt about it. We have seen in great detail how many problems this causes:

- everybody on Earth is considered a thief and is forced to pay many times for this "guilt" [**23**]
- it is almost impossible to become a full time artist without paying significant fees to people who didn't contribute in any way to the creative works which influenced your own creations [**15**]
- cheap digital devices which may be used in many legal and innovative ways are artificially castrated and reduced to fancy television sets [**17**]

Abolishing copyright altogether just because it is heavily abused, however, would really be throwing the baby with the bathwater. Lobbying to reduce its extension and limit its scope, instead, as well as only voting candidates who commit to do the same, would be surely enough to restore balance. As long as people don't forget to do it soon, of course.

Demand open technologies and research in, and from, Public Institutions

Public Universities are paid, at least partly, by taxpayers money and have a public mandate. Why not demand, then, that the software teachers in such institutions develop open formats and software with their students, so that it can be re-used in the common interest at the smallest possible cost for all citizens? The same applies to any Public Administration: such organizations should be, at the very least, obliged to share the software they produce at no cost among themselves, to avoid two departments paying two different developers twice to build from scratch two different (possibly incompatible) programs on two separate occasions, that do the same thing! Public Administrations should also, whenever they publicly release software, do so under an open license.

When it comes to using general purpose software already developed outside the organization, the two first and non-negotiable goals of a Public Administration must be:

- to guarantee that all public digital documents will remain completely readable in the near and far future and
- **never** impose the use of the same software programs they themselves use, on external partners, suppliers or all citizens

The first goal is what makes it possible to finally abandon the Papyrus age [**8**]: the second is an essential condition for protecting and increasing competition in the software industry and guaranteeing all citizens the chance to interact via computers with the Administration **they** elect and pay, at the smallest possible cost.

Both goals can and must be achieved imposing the use of open, "Free as in Freedom" file formats and communication protocols.

This is not the only condition, just the only one within the scope of this book: there is no ethical or technical reason, with the exceptions discussed below, to enforce the use of any specific operating system or software program.

It is certainly right to punish those who create a monopoly or violate the law abusing their dominant position. However, actions limited to allowing or limiting the ways by which vendors of proprietary software can bundle all their products to make competition impossible, does very little to prevent the current offender, or the next wanna-be monopolist from doing the same rather more subtly, as soon as possible. The right solution to preventing these cases is to realize that it is finally time that governments accept and deliver documents only in non-proprietary formats. This should be done because it **is** the right thing to do, not to punish any company. In this way everybody would be really free to use or not, any software product: monopolies would be impossible. Luckily, this has already started to happen in many countries [**49**], but it really needs the support and votes of all citizens.

The exceptions

The main cases where it is essential that only Free as in Freedom software [**38**] is used by Public Administrations are:

- teaching of basic Office Automation and, above all, Computer Science and ICT offered in Public schools or paid with public money anyway
- national security: only source code [**37**] which is continuously under public scrutiny and is always available and customizable at will without paying fees or accepting other conditions by one single (possibly foreign) private company is acceptable in, for example, military servers

Other examples of laws to fight Digital Dangers

Here is a short list, by no means complete, of laws that all citizens could ask to their representatives to vote and implement:

- Demand that the ICT budget of Public Administrations, schools and Universities goes for open operating systems and hardware, unless it can be demonstrated that there are only commercial alternatives
- Demand that all information on public spending is published online [**26**] and then, of course, get a computer and check it!
- Limit goverment support of schools and Universities using proprietary software whenever there are other solutions
- If no open solutions are available for word processing and other basic computers related tasks, finance their development in the shortest possible time

- Demand that all educational software, digital reference manuals or electronic encyclopedias, be they commercial or Free, can be used in public schools and Universities only if they are available for all operating systems
- Forbid or limit exclusivity agreements between hardware and software makers
- Impose that, on all new computers, hardware and software are priced separately and explicitly, and that all new computers can also be purchased, with the same financing conditions and warranty, without any software included.

There are two things in common among all these proposals. One is preserving public records which are really accessible to everybody, now and in the future. The other is the fact that guaranteeing equal opportunities by placing fair, competent rules on software and digital technologies can reduce public expenses and help the environment while creating more local jobs. No political party should refuse to grab such opportunities or to explain why it doesn't. It is time that very clear positions on these issues (and all the other Digital Dangers) begin to be always included in the program of **every** candidate to any political post, no matter what his or her party is: be sure to check them the next time you vote, and vote accordingly.

Where Are Consumer Associations?

Anybody who really cares about the real interests of all consumers can no longer ignore the existence, quality and advantages of open digital technologies because, as this book proves, their presence or absence directly impacts the wallets and quality of life of *all* citizens. Where then are all the Consumers Associations? Are they doing all they can, or anything at all, to inform and protect their members and all the other citizens from the Digital Dangers described in this book?

So far, in many countries this has happened only by chance, in isolated cases: not as a continuous, conscious and coherent strategy to be internationally coordinated. It is still pretty common for these groups to buy the first computer they find at the corner department store without thinking about its content, and then use it to write, in closed file formats, reports which will be published (maybe...) on websites not usable by all consumers [**27**]. This is not acceptable anymore: just as has been indicated for political candidates, even Consumer Associations should have an explicit policy of monitoring Digital Dangers, protecting their members from such dangers and spreading the necessary information.

Chapter 45

Make sure that Public Websites are Done Right

Every country has its own stories of huge amounts of public money wasted on services which were never obtained or could have cost much less. What is still little known among the general public is the fact that, unlike in recent years, websites have joined the list of public services which can be very expensive if they aren't Done Right [**45 - 1**].

As far as we are concerned here, "Done Right" means both "usable by any citizen, including people with disabilities, no matter which computer and Internet browser they use" and "not wasting taxpayers money".

This is a very important issue for two reasons. The first is that, apparently, to be an active and empowered citizen one must really go online these days. We are going towards a point where some services will only be available via the Internet. Not accessible or generally unusable public websites will waste more and more people time in the next years if they aren't managed properly.

The other reason to be concerned is that we are not talking of pocket change here. All governments are already spending a **lot** of your money on nifty websites and Internet based services.

In May 2006 just revamping the website of the British Department of Trade and Industry(DTI) cost at least 175,000 Pounds! Beside the price, the result was so bad from the accessibility point of view to raise very loud complaints from professional web designers [**45 - 2**], even after an official explanation from DTI on how the website had been commissioned [**45 - 3**].

The tourist portal Italia.it [**45 - 4**] was started in 2004. In December 2006 the website cost had already reached several millions Euro (45 according to some sources) but it still contained nothing more than a "coming soon" page [**45 - 5**], prompting requests for official investigations [**45 - 6**]. When it finally opened, in February 2007, there still were enough doubts on how the portal is managed and its lack of accessibility to prompt the creation of a website fully devoted to investigate and reports on the matter [**45 - 7**].

Of course, the case of Italia.it is an extreme one and only part of those millions Euro are due to hardware and software choices. The general trend with most public websites, however, is the same worldwide: any Administration must have at least one website (which is a good thing, of course), but this very seldom happens in the right way. In theory, there should be no problems: laws and regulations which specify guidelines for accessibility by disabled users and other requirements of all public websites already exist in several countries.

In practice, very often nobody inside a Public Administration has the will, the technical expertise or the authorization to demand and above all verify that the web design company which won the contract for the official website fulfilled all the relevant accessibility and usability regulations at the smallest possible cost.

All those rules are worthless if the designers and their customers, that is the Public Administrations which need a website, are not held accountable to them. Sometimes this happens even when the initial, official requirements for the website *were* compliant with such rules. The situation, however, is not going to change soon without real public pressure from voting citizens.

Even ignoring money savings, well done public websites may deeply transform Public Administration, making their services much faster and easier to use, even from home.

Public websites done in the wrong way, instead, may become a really meaningful source of waste of public money in the next years if citizens don't realize as soon as possible how much time and stress they could save with a decent website or how much of **their** money what looks like just a few screenfuls on a monitor can actually cost. Remember that even people who don't use public websites or don't own a computer in the first place pay these costs through their taxes.

How to act

Public websites, paid with public money, should be affordable and accessible to all citizens, including users with disabilities, not just the computer maniacs who spend half their income on a new computer every six months. These websites should be routinely tested, instead, with a two-year-old computer, the *slowest* Internet connection available and a text-only browser, to check how much information remains actually usable!

Do the websites of your schools and all your national or local Administrations pass these tests? If not, the right way to make this change is to complain and make pressure so that all existing public websites become Done Right [**45 - 1**], or that all new ones are designed from scratch as such. Just remember to do it on paper, through normal email, since the politicians who let these things happen may be unable to read any email. Besides that, one paper letter or fax is worth 10,000 email messages, because it's still perceived as much more real.

To find out or denounce which public websites still waste public money without providing the best possible service you can also visit the section of the Digifreedom website specifically devoted to this purpose.

As food for thought, what if it were required by law that **all** websites (yes, even personal ones!) publish online a list of all the software they used for the creation of every document they put online, license numbers included? Such a measure would do a lot to fight illegal software usage, at least for some classes of programs.

Of course, if applied to personal web pages it would be extremely difficult to verify that such a law is respected and doing so could also raise privacy issues which are better avoided. Imposing these rules on business and Public Administrations websites would be an entirely different matter, however, something which could do a lot to fight that part of software piracy which is used to publish a lot of material online.

Chapter 46

How Can A Parent Fight Digital Dangers?

Very often a computer, unlike purely passive appliances like TVs and DVD players, is not a luxury today. Without owning a computer or being *actually* competent in Information and Communication Technology, in many countries it's already much harder, if even possible, to graduate, find a good job and above all keep it. Everybody can play at will with his or her own money. No family, however, should be forced to dismiss a working computer and shell out more money just because a new home-banking website or some new software (new as in "can handle Etruscan fonts", not as in "it does something else **I** need") necessary for homework requires twice as much hardware and electric power. Equally important is to protect the digital future of your children.

Let children be hackers and protect the environment

Don't be fooled by the critical distinction between mere technofashion and conscientious use of technology. Sending SMS messages all day, chatting online or being able to set the correct time on a VCR has little or no added value at all, if that's all the technology a child or teenager are doing. Learning as soon as possible to look (and tinker) under the hood is one of the best technical and civic education lessons one could learn.

Being able to build things yourself has always been very popular among kids. Learning soon enough that one can (and should) be able to fix broken engines, that is to actively solve problems by him or herself rather than complain or sheepishly open his or her wallet is also essential to one's success in adult life, in every field.

Let's then just change the engine to look at, i.e. let's *encourage* our children to open computers and their software, rather than the hood of a car. It's much cheaper, much more important, much more powerful and much more environmentally sustainable. On top of that, it's even much cooler, today.

Teach children to be fair and fight copyright abuse in the right way

Many children and teenagers probably still violate the law every day. The same kids everybody is so proud of: Eagle Scouts, school team pillars, Parish choir leaders and so on.

Illegally installing music, video, games and software is one of the most useless, that is stupid, crimes ever. It is wrong, and potentially dangerous, to educate your children to violate laws just because you or they think they are stupid; at least in all cases where there is really no threat to survival (that is you are not left without food, medicines, shelter or basic schooling) and, above all, viable and perfectly legal alternatives **do exist**. Copyright abuses *must* be fought, but in the right way. Illegal copying gives corporations the best excuses they could ever dream of to block children from **becoming** artists or authors tomorrow, without signing some contract that enslaves them to somebody else's stock options. Let's explain to children that it's much smarter and more fun to follow *other* paths. Please leave the corporations without the pretext to make many uses of technology illegal or practically unfeasible, uses which are essential to get a good education or job or to exercise basic civil rights.

Last but not least: let's urge children and teenagers to convert their audio and video files as soon as possible to free multimedia formats [**40**]. After getting rid of all the illegal material from the computer, of course.

Let children create

Music and art in general are essential. If you worry about how much money your children would spend on music, or they nag you about it, do the right thing: buy them a nice guitar, one of those old fashioned things that happily play without electricity, even in the middle of the woods, and take them there, to play and have a good time.

There is no question that children and teenagers alike should be encouraged to be active, to express themselves, to engage in constructive discussion and to share their feelings with others. A proper use of Free Software at the right age is a very economical, cool and powerful way to achieve these goals: even a two or three year old computer can be an excellent tool to compose music on, draw stunning 2 and 3-D graphics, write poetry, fiction, and much more. They also get top notch computer training through a process which also teaches the value of cooperation and how to work in team efficiently.

In short, let's teach kids to respect the work of others even when it's digital, but also to try to create themselves. Of course, being creative with computers should still come after [**10**] old-fashioned education and interaction with one's neighbors and classmates. There is little point in being pals with lads living ten thousand miles away if a child still doesn't know the name of the next door neighbors, and couldn't care less if they live or die.

Protect their future opportunities

Let's give children laws that make it possible, that is both legal and affordable, to be creative artists, authors, performers or hackers tomorrow with as few intermediaries as possible. The right way to make this happen is that all parents start requiring as soon as possible from their lawmakers a fair copyright and a really fair use [**18**] of creative works.

Protect children's privacy online... in the right way

Websites devoted to making as many friends as possible online, to share anything from pictures to hobbies and contact information, are very popular and easy to use nowadays. It is certainly possible that a minor gives out enough personal information on these websites to put him or herself in concrete dangers of all kinds. For this reason there have already been several proposals for laws in some countries to force all these websites to verify users' ages and get parental authorization [**46 - 1**] before allowing minors to publish anything online.

Surely such proposals can help and are made with the best of intentions, but they have two big limitations which is essential that we do not overlook. One is that there are no technical procedures which are both practically feasible and hard to circumvent. The other is that principles and common sense must be first tought and practiced in the family. Law and technology can only assist parents, not replace them.

Don't tolerate illegal software in or from schools

This can also be a very effective way to distinguish the educators who really care about their pupils and those who only live for the next paycheck, and look at teaching as if it were no more critical than stacking paper. It is essential to demand that schools:

- explain to the students that there **is** software that can be legally installed and duplicated at no cost [**38**].
- exchange computer files in proprietary formats only when there is really no open alternative.
- (when proprietary formats cannot possibly be avoided) do not allow students to deliver files in those formats, if they cannot prove that they created them with legally installed software.
- teach software design using Free Software [**38**] to the maximum extent possible

- set up and support, if the budget allows it, sharing of student-produced content, and content which can be legally shared. There already is a lot of it [**46 - 2**] online
- follow the advice in the next chapter of this book

Also remember to take advantage of the database of Digitally Free Schools [**47**] and contribute to it.

Chapter 47

How to recognize a really good ICT School Program, and why

Regardless of its actual cost, sending a child to a good school is always a huge investment in the future. The relevance, inside school programs, of Information and Communication Technology (ICT), that is how to correctly use computers or telecommunications devices for fun and profit, is constantly increasing. This is a good and necessary thing, even if often it is done just to be trendy and some families are tiring of it [**10**].

Now, how can a parent recognize the best ICT package for his or her children? How can one figure out if it will still be worth something by the time one graduates? Does the answer require any specialist knowledge? Luckily not!

The right questions are below. They are valid for any scenario from primary school to University degrees or single-purpose private courses or Professional Schools. Ask those questions, decide according to what you discover and, above all, if you decide not to go to a particular School or University for the reasons below, do take the time to let that Institution (and all the newspapers and TV stations in their area) know **why** you chose to go somewhere else.

The bogus ICT program checklist

Money first

The computer technologies used in schools, especially public ones, must not discriminate against the less wealthy children, by forcing their families to spend unnecessary money. If the expense for parents is null because already included in the school tuition or paid for by the Government, those are just more reasons to make sure that no money is wasted.

Who pays, and why?

There is nothing wrong with a computer class supported by a private company with any combination of its money, teachers, software or hardware. It is perfectly logical and legitimate to do so, both for the company and for the school which is funded, but only if the program is balanced, the (public) school mission is not forgotten, and no software time bombs [**3**] are placed in the life and career of the students!

Do the computer activities at school tolerate or induce illegality?

Education is about principles, isn't it? Well, as sad as it is, sometimes it is the teachers themselves who distribute the free drug, er we mean illegal copies of software programs [**47 - 1**] to their students, or indirectly force them to use such copies: this may happen because the school curriculum is structured in such a way (but who wrote it?) that there are no alternatives than to use those programs at home. So much for ethics.

Remember that, in such cases, providing free or discounted copies to students is in the interest of the software makers. If the course program forces the usage of their software, all the students who today have little money anyway will be much more likely to prefer that software when they start working. Then they'll be forced to pay whatever the full price is [**3**], and will obviously pass it on to their customers, that is, the rest of us.

Considering all this, does the school check that no student uses (both in the classroom and at home) illegally installed computer programs?

Sometimes, proprietary software is still the only kind of software appropriate for the courses in which it is used, as may still happen with some engineering programs. In such cases, are there enough computers in the school for all students to work on their projects during school hours? If the students are forced to used the same programs on their own computers, does the school takes care to get a special, hopefully free license for them?

If teachers receive homework that could have only been done with expensive software, do they ask for proof that the student obtained and used it legally [**36**], rather than inducing or tolerating illegal software usage?

Above all: do teachers know that there is software that can be legally installed for free and is more than adequate for the great majority of grade school projects?

Life expectancy of what is taught

No computer course program should focus on things that will be obsolete before the class ends. Many courses are sponsored, either directly or indirectly, by software vendors [**11**] who need to release a new version every other year to survive. Many schools are proud to teach you immediately *not* how to do something (writing, calculating formulas) but how to use the *latest* version of this or that software package.

Teaching specifically how to use **one** version of **one** program, even if it were surely the best one in its field, is really like, instead of teaching writing, schools showing students the healthier and most efficient way to hold the latest model of pen from only one maker. The only reason they can get away with this is that computers are still seen as some must-have incomprehensible black magic by most of us. More or less consciously, we think that we will never be able to ask for better treatment without sounding stupid, and anything goes.

Is this computer-related training? Certainly. Is this worthwhile education? Hardly, if the course program stops there. In that case, it would be a sure sign that the course is worthless. Chances are that one will not remember anyway, nor find valuable, most notions of this kind in one year from now. Most basic courses which want to be this specific should come at no cost for their end users (online or in DVD/videotape form, maybe), with the software itself, if they already paid to use it.

By the way, the same judgment applies to all those job offers which demand "perfect knowledge" of *specific* versions of office productivity software (word processing, spreadsheets etc). Stay away from those companies if you can.

Concepts or buttons?

Do they teach what the problem being studied is (accounting, word-processing, whatever) and how to solve it in general? Do they teach how to install, set up, upgrade, troubleshoot and customize the software appropriate for the task, or just to click buttons like a monkey?

Why worship mouses and windows?

The advertising of many computer courses is based on some combinations of these two slogans:

- "This shortens the learning curve" (that is the time before you can do something with the software all by yourself)

- "This has a graphical user interface, no need to know and type arcane commands"

These sentences sound like life savers. It's like being beamed by aliens up to their planet and discovering you **can** talk to them with just some simple gestures. On the other hand, if people went from sign language and simple pictures to real speech and alphabets and never went back there must be a reason.

Learning just the bare minimum of graphical interfaces is perfectly acceptable and honorable for irregular and basic computer usage. If we all were software programmers, how boring would life be? There are also a lot of situations when a nice graphical interface is the best, if not only way to go. Landscaping, Computer Aided Design (CAD) or photo editing are just a few examples. A mouse-only approach, however, can be extremely limiting.

"Short learning curve" very likely implies that it will be impossible, or very difficult, to ever do more than one can learn in the first two months. "Point and click graphical interface" often means that you cannot automatize anything. When moving a computer mouse is the only way to do something, a human must remain attached to it all the time: the mouse cannot memorize complex or repetitive instructions. Real computer education, instead, should teach how to spend as *little* time as possible in front of a monitor. If you *can* save one digital photograph in just two clicks, but *must* manually click two hundred times to save one hundred pictures, you can't afford long vacations to take pictures!

Again, there is nothing intrinsically wrong with refusing to learn all the secrets of every program you encounter, if it is for fun or really limited needs. Software is just a tool, not a religion. But sending anybody's education and career down a "point and click all the way" route is really risky and unfair. If all that is known or offered by the job market are mouse click sequences, there will always be cheaper countries where those clicks can be outsorced.

What is the other way to do it?

This is strictly related to the three previous questions. In order to make sure that the skills you pay for will be valuable in real life, a course in any discipline should teach at least two different ways to solve the same problem. In many software-related classes this means introducing at least two competing programs. If this doesn't happen, what is the reason why not? Is it because there really are no competing programs, or because the teachers are not prepared to explain them both? Or is it because the teachers are not required nor encouraged to do so?

The European Computer Driving License

Many countries have already instituted and started to offer, or require from all applicants for public employment, some basic Computer Knowledge certification. One of the biggest and most important initiatives of this kind is the European Computer Driving License (ECDL) [**47 - 2**] which also exists in an International version (ICDL). The concept behind the ECDL is to guarantee that the minimum skills necessary to work with computers, as well as the qualification of the instructors, are fairly and clearly defined.

As many other Government-sponsored initiatives, the ECDL and similar programs could become an excellent occasion to improve general education, as well as a wonderful opportunity to spread better and less expensive software [**47 - 3**]. There are equal odds that the whole thing may become yet another cultural disaster and huge waste of public and family money. The greatest risk is that all the Government funding for ECDL and ICDL ends up aggravating public debt to the advantage of a few multinational companies.

Stay away from ECDL and similar courses when they don't pass the test described above. Ask their organizers, and the Government branches which fund them, to stop such a misuse of public money. A State-funded program for large scale ICT education cannot simply teach how to click buttons, perpetuating (with public money!) the dependence from overpriced software.

The Database of Digitally Free Schools

Finding or advertising Schools and Universities which protect the Digital Freedom of their students and their families will hopefully become much easier in the near future. The Digifreedom.net website has started a searchable database **[1 - 4]** where all schools can describe how their ICT offer guarantees Digital Freedom, as described here and in the other chapters of this book. On the same website all students and parents can add comments and exchange their experience on any school listed in the database.

Chapter 48

How All Internet Users Can Fight The Digital Dangers

Today we are all ”users”, or at least unconscious sponsors, of the Internet and digital technologies, even if we do not use yet a computer or an Internet connection: all the true stories mentioned in this book demonstrate this fact. This said, can a simple (maybe unwilling) user, somebody who only needs to use computers and the Internet in a very basic way contribute to making the Internet a Better Place? Of course: here's how.

To begin with, let's avoid like the plague all the web-based services and applications [**28**] which are not already guaranteed to work across all types of software and hardware devices, from traditional computers to cell phones. You never know which kind of terminal may be the only one available to check your bank account or contact your manager when you're traveling. Next, use only standard compliant browsers like Firefox [**48 - 1**] and whenever a site and/or the documents it makes available for download, are usable only with proprietary software, do the following two things.

First, let them know that you won't come back, and why. This is the most essential thing. Websites live off traffic: never visiting a bad one again, after letting it know why, is the fastest way to solve the problem: make yourself heard, since just ignoring them will perpetuate the problem. If you can find their email address (yes, many communication-challenged guys still set up web sites without giving you contact info), use it. If you don't find it try wemaster@the.closed.website.address. Send the message to newspapers, too, or maybe only to them if you fear it's a site that could spam you. Alternatively, you could get a second email address, to be used only via web for these purposes. If you **run** a website, you may also consider joining the Website Done Right campaign [**45 - 1**]!

The second thing to do is to never build bad websites. Internet communication is **not** supposed to be "best viewed in such-and-such a resolution, or only with such-and-such a browser, or with a link speed not less than X".

If you need a website and hire professionals to take care of it, or just ask it as a favor to some web-savy friend, require that they always use, at the very minimum, open, non-proprietary file formats which are **guaranteed** to work on every computer: both for web pages, and for every documentation that's put online for your visitors to download.

Also make sure your webmaster isn't one of those who must put animated pictures, sound effects, mini-movies or other gadgets on every page, even when they are not needed, simply to justify their salary. Stay away from those people. Do it. Ninety nine per cent of your likely visitors will have computers or Internet enabled cell phones which are different, or differently configured from yours, or slower connections: you can't bother them like this. They want to talk, not just listen, i.e. be active, not passive. Maximize the speed at which they can use your website, instead of generating more trash TV.

There is a short, absolutely non technical list on the Digifreedom website which can help you in two ways: to choose the right webmaster for your business and to make sure that he or she does what is needed in the right way.

Chapter 49

What Are Other Countries Doing?

A lot, even if it isn't the kind of news which, until today at least, was likely to make the front page of the Enquirer. The following list, while very incomplete, should be more than enough to convince any parent that Free protocols, file formats and software are taken really seriously, are already moving or saving a lot of money and should be available and familiar to every child who should have all the possibilities to go far in the world.

Free software worldwide

China, Japan and South Korea announced an official initiative in 2003 to promote open source software and platforms such as Linux [**49 - 1**], in order to increase their self-reliance in the Information Technology sector. In January 2007 the Government of the Indian State of Kerala proposed to make the State as "the Free Software destination in India" [**49 - 2**], establishing an International Center to develop Free Software technologies for social and economic advancement in developing countries. The policy proposal also includes the will to use OpenDocument [**41**] and similarly open standards [**40**] just to avoid total dependence on a few software vendors. Vietnam has a Master Plan for "applying and Developing Open Source Software for the 2004-2008 period" [**49 - 3**]. Starting from summer 2007, members of the French Parliament and their assistants will use the Ubuntu version of the Gnu/Linux operating system [**49 - 4**].

Are open formats coming?

They surely are raising more and more interest every day worldwide, in all fields. South Korea announced in May 2006 an overhaul of its national mapping system [**49 - 5**] using open standards and software. Three months later, the Hong Kong Government recognized OpenDocument as the recommended standard for interoperability [**49 - 6**] in the areas of collaborative editing of texts, presentations and spreadsheets. In the same month, the Danish Open Source Business Association estimated that the State and local Governments could save about 94 million US Dollars by migrating to OpenOffice.org and OpenDocument [**49 - 7**]. One year before, the Norwegian Minister of Modernization had announced that his government "eNorge 2009" plan includes a transfer to Open Source by 2009, when "Proprietary formats will no longer be acceptable in communication between citizens and government" [**49 - 8**]. As of March 2007, the "Precedents" page of the OpenDocument Fellowship, a volunteers organization devoted to OpenDocument promotion and development, lists almost forty countries where at least one central or local government body has decided to adopt office software supporting OpenDocument [**49 - 9**].

Does it always work perfectly?

No. There are cases, like the one of the Berlin Senate, which in June 2006 opposed a complete migration to Free operating systems [**49 - 10**] after the software migration trials didn't go smoothly. Actually this is a good proof of the fact that, when proprietary communication protocols and file formats are used, software, like nuclear plants, is dangerous even after you stop, or try to stop, using it [**3**]. What matters more then it is to *accelerate* the transition to freely usable protocols and formats, to minimize the damages and put an end to them as soon as possible.

What about Copyright?

Luckily, even the copyright-related laws and regulations which contribute so much to create the Digital Dangers or extend their scope are starting to irritate some public officials, at least apparently. In March 2007, for example, a European Union Commissioner asked if it's reasonable that a song purchased from one digital store cannot be played on any digital music player, adding "It doesn't to me. Something must change." [**49 - 11**] In 2006 the Consumer Council of Norway filed a complaint against just this kind of practice. Similar initiatives are under discussion in several countries, but they may not see the light soon enough to be useful, if they aren't backed by popular pressure.

What does all this mean?

It is especially interesting to note that many of these initiatives are not happening in countries which have been the most technologically advanced so far, but in those who are catching up, free of the burdens of false starts and antiquated infrastructures so common in "first world" countries.

In many emerging countries a very large percentage of software programs is distributed and installed illegally. This is not going to continue forever, though. Partly, it is for ethical reasons, and partly because there is no point in stealing the apparently latest and greatest software if it still forces you to buy a much powerful computer just to boot up. Emerging countries have less money to waste and therefore are more motivated to find the really efficient solutions, that is to go in the right direction earlier.

Another important point is that many of these initiatives don't come from hating the free market or anything similar. In most cases they don't actually care about which software is used. They simply want to make sure that unrestricted access to public records

[**8**] in their original electronic format is possible even many years after the documents were created. This can be guaranteed only using non-proprietary communication protocols and file formats. When it comes to actually mandating the usage of Free Software [**38**], usually the reasons are purely technical, like the fact that it is essential to spot backdoors or privacy violations, and to not leave public offices depending on one or very few vendors.

In any case, all the facts mentioned in this chapter demonstrate that this is the right moment to fight all the Digital Dangers at the State level and that many countries are already doing it, or trying to do it, to jump ahead of the others. Even more importantly, these facts prove that it is essential, for any Government which cares about minimizing expenses, maintaining control of its own culture and data, and creating (and keeping at home) as many qualified jobs as possible to not remain behind in this particular race.

Chapter 50

Living among digits and hackers: survival tips

Breaking the last wall

The main obstacle to defeat the Digital Dangers is maybe the lack of communication between average parents and average hackers. Sometimes it is just difficult to grasp the connection between abstruse issues like software development or copyright reform and one's concrete, ordinary life. In a few, extreme cases, the first encounter with the Free Software "activists" may have been an unhappy one: *"I tried to ask for help from the Free Software community one or two times, and all I got were insults, or no answers at all"*.

There is no problem to leave the actual design and implementation of software to real, competent programmers. What is wrong, when civil rights and education are concerned, is if those programmers ignore the actual point of view, needs and possibilities of everybody else, or abuse ordinary users because of their technical skills. Bad manners and narrow points of view can never be excused, even when they come from some genius. There is also no reason to feel inferior to a technical expert, when the problem to solve is an ethical one.

At the same time every software user, no matter how "technologically challenged", must learn at least to read the manuals and ask online for help in the proper and most effective manner if he or she wants to use a computer or generally fight the Digital Dangers.

This said, parents, teachers and hackers all need to learn the right language to interact with each other and start doing it soon. Parents and teachers, more than everybody else, also need to do their part as soon as possible for a better digital society. Hackers must not be free to feel superior, but they should really be kept free to do their work, and in this sense it is essential that everybody makes pressure for the right laws to be adopted worldwide.

What matters is to finally *start* talking to each other. The reason is the one stated at the beginning of this book: today the quality of everybody's life, not just that of programmers, heavily depends on which software is used **around** them. The modern world is too dependent on digital technologies to keep ignoring these issues.

How the Digifreedom website can help

The Resources section of the Digifreedom website will soon host practical instructions, suggestions and pointers to the best resources on how to install and use Free Software, from how to try it at home **without** installing anything to how to get technical help in the most effective way or how to shop for FOSS service contracts. You will also find links to tutorials on how to minimize or avoid the risks of using a computer in the family, restricting or monitoring usage of the Internet only if and how you, not the government, think is the right way to act. There will also be forums to discuss and protect Digital Freedom together with other parents and teachers.

Besides a directory of Digitally Free Schools, the website will also host a list of bad public websites and another one of mainstream media outlets which have demonstrated poor or no knowledge when covering the issues discussed in this book.

Once you have became more familiar with these issues and (hopefully) contacted other concerned parents or teacher through the Digifreedom website, the next move to establish a contact with

Free Software or Free Culture activist and work together may be to find the Gnu/Linux User Group closer to your neighborhood and arrange a meeting with them to start fighting the Digital Dangers together. GNU is a recursive acronym which stands for "GNU's Not UNIX" and indicates the completely Free as in Freedom computing environment whose development was launched by Richard M. Stallman in 1984. Linux is a Free as in Freedom kernel, that is the basic software program inside each computer, the one which starts and coordinates all the others. Gnu/Linux systems are the easiest and most popular alternative to Digitally Dangerous software environments.

Another useful move would be to contact the closest office of two international organizations which are very active in this area, the Electronic Frontier Foundation [**50 - 1**] and the Free Software Foundation [**39 - 1**].

Conclusion: act and spread the word

All the Digital Dangers described in this book are interrelated global problems which require local pressure to find a proper solution.

Today there are still many differences which make some countries less Digitally Dangerous for their citizens than others, but there is also a very strong political pressure to make such countries conform only to the interest of software and entertainment multinationals. There is, for example, an official blacklist of countries that are believed to be persistent offenders of copyright, patents, trademarks and other related regulations [**C - 1**]. In the long term, having the same or very similar laws in every country is unavoidable in some fields and it is also (potentially, at least) a good thing. This is true, however, only if **all** citizens push to make this standardization happen in the right way for the *common* good.

What now?

This book does not and cannot contain complete descriptions of each Digital Danger and its solutions. More exactly, some specific technologies mentioned in this book are still very young and in active development, so it may very well be that they turn out to **not** be the best solutions. That's no problem.

What matters is to be aware that all the issues discussed in this book are *already* affecting your life and that of your children. Reading this book is just the first step. Its main purpose is to help all parents and teachers to understand that, unless they start acting today to protect from the Digital Dangers their own interests and civil rights, together with those that their children may not have tomorrow, adequate legal and technical solutions will never be developed and used.

It is also important that you don't feel scared or intimidated by technology. Remember: in many cases, you don't even have to use it yourself unless you wish to: you just have to make sure that its usage is regulated in the best possible way. Common sense, a bit of good will and a sense of responsibility are all you'll need to achieve good results.

If you still feel scared and intimidated by the digital world, remember that your political representatives at any level are probably in the same boat as you are, but *their* task is to solve *your* problems, even in this area. Let them know without doubt that you will also consider how they fight Digital Dangers before voting the next time.

In any case, no matter which way is the best for you and your family, please act and spread the word!

Don't forget that there are forums and further information, links and other resources at the Digifreedom website. Please use them also to let me know what you think of this Guide and of the Digital Dangers, how you plan to fight them and what help you need to do it more effectively.

Marco Fioretti