

The Right to Read

by **Richard Stallman**

This article appeared in the February 1997 issue of Communications of the ACM (Volume 40, Number 2).

(from “The Road To Tycho”, a collection of articles about the antecedents of the Lunarian Revolution, published in Luna City in 2096)

For Dan Halbert, the road to Tycho began in college—when Lissa Lenz asked to borrow his computer. Hers had broken down, and unless she could borrow another, she would fail her midterm project. There was no one she dared ask, except Dan.

This put Dan in a dilemma. He had to help her—but if he lent her his computer, she might read his books. Aside from the fact that you could go to prison for many years for letting someone else read your books, the very idea shocked him at first. Like everyone, he had been taught since elementary school that sharing books was nasty and wrong—something that only pirates would do.

And there wasn't much chance that the SPA—the Software Protection Authority—would fail to catch him. In his software class, Dan had learned that each book had a copyright monitor that reported when and where it was read, and by whom, to Central Licensing. (They used this information to catch reading pirates, but also to sell personal interest profiles to retailers.) The next time his computer was networked, Central Licensing would find out. He, as computer owner, would receive the harshest punishment—for not taking pains to prevent the crime.

Of course, Lissa did not necessarily intend to read his books. She might want the computer only to write her midterm. But Dan knew she came from a middle-class family and could hardly afford the tuition, let alone her reading fees. Reading his books might be the only way she could graduate. He understood this situation; he himself had had to borrow to pay for all the research papers he read. (10% of those fees went to the researchers who wrote the papers; since Dan aimed for an academic career, he could hope that his own research papers, if frequently referenced, would bring in enough to repay this loan.)

Later on, Dan would learn there was a time when anyone could go to the library and read journal articles, and even books, without having to pay. There

“The Right to Read” was written to illustrate a worst case scenario future, which might happen if the current trend in copyright legislation is continued. The scariest aspect of the story is that it has, in the USA at least, mostly already happened. That is, it has happened in law. There are two reasons it has not happened in reality: they are not strictly enforcing the law, and much of copyrighted material is still in analogue form.

If Bill C-61 passes, nearly all of the dire predictions in this story will come true in Canada as well — if we choose to enforce the new law. Will Canadians stand for that kind of enforcement? I very much doubt it, but I would rather not have these laws on the books.

There are already venues of reading that function like this. If you buy a digital book from Amazon.com for their Kindle device, there is no legal way to lend it to a friend, except possibly to lend your entire Kindle. Books cannot be displayed on other Kindles unless they are registered to you. It is possible to bypass these restrictions, but this violates Amazon's terms of service (which Bill C-61 says trump any fair use rights), as well as C-61's anti-circumvention provisions. Other online bookstores are similar.

References:

Amazon terms of use for the Kindle:

<http://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=200144530>

Relevant C-61 sections:

17 (amending Copyright Act 29.2, which protects “Fair dealing for the purpose of research or private study”)

“copyright monitors”: this already exists in music CD's. At least one company (Sony BMG) used a hidden computer program that would install itself without any indication that it was doing so. The program would then prevent the user from making copies of the CD (no matter what the intended purpose), as well as taking the sinister step described here of “phoning home” to Sony BMG. Attempting to remove the software resulted in the CD drive being totally disabled.

Needless to say, this produced a consumer uproar and Sony BMG no longer uses this particular method of copy protection. That doesn't mean, however, that they were ever found guilty of breaking any laws.

In fact, if C-61 passes, this kind of underhanded “technological measure” might not only be allowed, but consumers who find ways of disabling it may find *themselves* liable.

References:

http://en.wikipedia.org/wiki/2005_Sony_BMG_CD_copy_protection_scandal (look at references from “Mark's Blog” for a complete technical explanation)

Relevant C-61 sections:

31: Amending section 41 of Copyright Act

A “slippery slope” argument:

Bill C-61 contains special exceptions for libraries that exempt them from the penalties for bypassing “technological measures.” (**C-61 section 31**, amending section 41.19 of Copyright Act) and other provisions of copyright (**C-61 section 32**, amending Copyright Act section 42). In fact, libraries are required to take “technological measures” of their own to prevent patrons from “making any reproduction[s] of the digital cop[ies]”, “communicating the digital cop[ies] to any other person”, “using the digital copy for more than five business days” (**C-61 section 20**, amending 30.2(5) of Copyright Act). Since these provisions are only enforceable if the library (or some other entity) has prevented patrons from having complete control over their computers, there is in fact no way libraries can satisfy these requirements. If the the lobby groups responsible for this bill win, it is only a matter of time before libraries are only allowed to keep paper items, or are ruled outright illegal. Having to make explicit exceptions for libraries means that the bill as a whole is too restrictive, and making those exceptions is half the process of being able to revoke them later.

were independent scholars who read thousands of pages without government library grants. But in the 1990s, both commercial and nonprofit journal publishers had begun charging fees for access. By 2047, libraries offering free public access to scholarly literature were a dim memory.

There were ways, of course, to get around the SPA and Central Licensing. They were themselves illegal. Dan had had a classmate in software, Frank Martucci, who had obtained an illicit debugging tool, and used it to skip over the copyright monitor code when reading books. But he had told too many friends about it, and one of them turned him in to the SPA for a reward (students deep in debt were easily tempted into betrayal). In 2047, Frank was in prison, not for pirate reading, but for possessing a debugger.

Dan would later learn that there was a time when anyone could have debugging tools. There were even free debugging tools available on CD or downloadable over the net. But ordinary users started using them to bypass copyright monitors, and eventually a judge ruled that this had become their principal use in actual practice. This meant they were illegal; the debuggers' developers were sent to prison.

Programmers still needed debugging tools, of course, but debugger vendors in 2047 distributed numbered copies only, and only to officially licensed and bonded programmers. The debugger Dan used in software class was kept behind a special firewall so that it could be used only for class exercises.

It was also possible to bypass the copyright monitors by installing a modified system kernel. Dan would eventually find out about the free kernels, even entire free operating systems, that had existed around the turn of the century. But not only were they illegal, like debuggers—you could not install one if you had one, without knowing your computer's root password. And neither the FBI nor Microsoft Support would tell you that.

Dan concluded that he couldn't simply lend Lissa his computer. But he couldn't refuse to help her, because he loved her. Every chance to speak with her filled him with delight. And that she chose him to ask for help, that could mean she loved him too.

Dan resolved the dilemma by doing something even more unthinkable—he lent her the computer, and told her his password. This way, if Lissa read his books, Central Licensing would think he was reading them. It was still a crime, but the SPA would not automatically find out about it. They would only find out if Lissa reported him.

a remark on “independent scholars” and the existing Copyright Act:

The existing Copyright Act contains provisions such as section 29.4, which grant educational institutions the rights to “make a manual reproduction of a work onto a dry-erase board, flip chart or other similar surface intended for displaying handwritten material” and suchlike — ordinary citizens are not granted these rights.

Effectively what that says is that ordinary citizens are prevented *by copyright laws* from teaching groups of others. (Granted, this is only the case if the materials and books being taught from are copyrighted, but given that nearly all books are copyrighted until decades after the authors die, it's a moot point.)

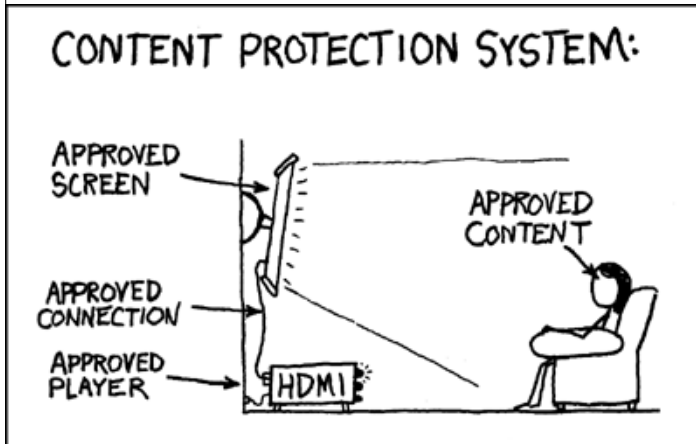
If we're going to amend copyright law, I believe this point should be addressed; education is after all a human right.

“debugging tools”: the story is correct, debugging tools can and are used to bypass “technological measures” protecting copyright (also called Digital Rights Management or DRM). They are also an integral part of computer programming. They are also illegal under **C-61 section 31**. The only way to resolve this conflict (if C-61 is allowed to become law) is to make it illegal for ordinary citizens to use debuggers and, eventually, to make it illegal for ordinary citizens to write computer programs.

All “technological measures” fundamentally rely on the user not being allowed to examine how they work. “Technological measures” protecting copyright differ from other forms of encryption or security in this way because, by their nature, they *must* be designed to allow *some* means of access to the material they are protecting. If users are allowed to observe how this means is provided, making the “technological measure” provide that means whenever and however the user wants is trivial. “Technological measures” for protecting copyright are fundamentally unworkable as long as people are allowed full control over their computers.

References:

http://news.zdnet.com/2100-9588_22-6189011.html (and many others...)



free operating systems: These do indeed exist, and the only way to play “protected” content on them is to break the protection. This is so because under the philosophy of free software, the programming code is freely available. Of course, this lets anyone see exactly how it works.

Playing DVD's on a computer running a free operating system has been technically illegal in the USA since they introduced their Digital Millennium Copyright Act, which, like Bill C-61, prohibits circumventing a “technological measure.”

Of course, if the school ever found out that he had given Lissa his own password, it would be curtains for both of them as students, regardless of what she had used it for. School policy was that any interference with their means of monitoring students' computer use was grounds for disciplinary action. It didn't matter whether you did anything harmful—the offense was making it hard for the administrators to check on you. They assumed this meant you were doing something else forbidden, and they did not need to know what it was.

Students were not usually expelled for this—not directly. Instead they were banned from the school computer systems, and would inevitably fail all their classes.

Later, Dan would learn that this kind of university policy started only in the 1980s, when university students in large numbers began using computers. Previously, universities maintained a different approach to student discipline; they punished activities that were harmful, not those that merely raised suspicion.

Lissa did not report Dan to the SPA. His decision to help her led to their marriage, and also led them to question what they had been taught about piracy as children. The couple began reading about the history of copyright, about the Soviet Union and its restrictions on copying, and even the original United States Constitution. They moved to Luna, where they found others who had likewise gravitated away from the long arm of the SPA. When the Tycho Uprising began in 2062, the universal right to read soon became one of its central aims.

Author's Note

This note was updated in 2007.

The right to read is a battle being fought today. Although it may take 50 years for our present way of life to fade into obscurity, most of the specific laws and practices described above have already been proposed; many have been enacted into law in the US and elsewhere. In the US, the 1998 Digital Millennium Copyright Act established the legal basis to restrict the reading and lending of computerized books (and other works as well). The European Union imposed similar restrictions in a 2001 copyright directive. In France, under the DADVSI law adopted in 2006, mere possession of a copy of DeCSS, the free program to decrypt video on a DVD, is a crime.

In 2001, Disney-funded Senator Hollings proposed a bill called the SSSCA that would require every new computer to have mandatory copy-restriction facilities that the user cannot bypass. Following the Clipper chip and similar US government key-escrow proposals, this shows a long-term trend: computer systems are increasingly set up to give absentees with clout control over the people actually using the computer system. The SSSCA was later renamed to the unpronounceable CBDTPA, which was glossed as the “Consume But Don't Try Programming Act”.

The Republicans took control of the US senate shortly thereafter. They are less tied to Hollywood than the Democrats, so they did not press these proposals. Now that the Democrats are back in control, the danger is once again higher.

In 2001 the US began attempting to use the proposed Free Trade Area of the Americas treaty to impose the same rules on all the countries in the Western Hemisphere. The FTAA is one of the so-called “free trade” treaties, which are actually designed to give business increased power over democratic

The remainder of this story deals with the way administrators of large computer systems (especially in universities) treat “suspicious activities.” This isn't really relevant to Bill C-61, so I'm not going to comment on it.

Following is an Author's Note, explaining the progress we've made towards this grim future since 1997. It references “trusted computing,” which unfortunately is pretty technical to explain, but it is happening. It is a step the copyright lobby and a select few large companies (who would be holding the reigns) need in order to have that complete control I mentioned above.

At this point many computers are equipped with parts of the “trusted computing” system, but those parts are disabled by default until the user explicitly turns them on (references: http://en.wikipedia.org/wiki/Trusted_Computing#Hardware_and_software_support and <https://www.trustedcomputinggroup.org/faq/>).

(End of Felix's commentary.)

governments; imposing laws like the DMCA is typical of this spirit. The FTAA was effectively killed by Lula, President of Brazil, who rejected the DMCA requirement and others.

Since then, the US has imposed similar requirements on countries such as Australia and Mexico through bilateral “free trade” agreements, and on countries such as Costa Rica through CAFTA. Ecuador's President Correa refused to sign the “free trade” agreement, but Ecuador had adopted something like the DMCA in 2003. Ecuador's new constitution may provide an opportunity to get rid of it.

One of the ideas in the story was not proposed in reality until 2002. This is the idea that the FBI and Microsoft will keep the root passwords for your personal computers, and not let you have them.

The proponents of this scheme have given it names such as “trusted computing” and “palladium”. We call it “[treacherous computing](#)”, because the effect is to make your computer obey companies instead of you. This was implemented in 2007 as part of [Windows Vista](#); we expect Apple to do something similar. In this scheme, it is the manufacturer that keeps the secret code, but the FBI would have little trouble getting it.

What Microsoft keeps is not exactly a password in the traditional sense; no person ever types it on a terminal. Rather, it is a signature and encryption key that corresponds to a second key stored in your computer. This enables Microsoft, and potentially any web sites that cooperate with Microsoft, the ultimate control over what the user can do on his own computer.

Vista also gives Microsoft additional powers; for instance, Microsoft can forcibly install upgrades, and it can order all machines running Vista to refuse to run a certain device driver. The main purpose of Vista's many restrictions is to make DRM that users can't overcome.

The SPA, which actually stands for Software Publisher's Association, has been replaced in this police-like role by the BSA or Business Software Alliance. It is not, today, an official police force; unofficially, it acts like one. Using methods reminiscent of the erstwhile Soviet Union, it invites people to inform on their coworkers and friends. A BSA terror campaign in Argentina in 2001 made slightly-veiled threats that people sharing software would be raped.

When this story was first written, the SPA was threatening small Internet service providers, demanding they permit the SPA to monitor all users. Most ISPs surrendered when threatened, because they cannot afford to fight back in court. (Atlanta Journal-Constitution, 1 Oct 96, D3.) At least one ISP, Community ConneXion in Oakland CA, refused the demand and was actually sued. The SPA later dropped the suit, but obtained the DMCA which gave them the power they sought.

The university security policies described above are not imaginary. For example, a computer at one Chicago-area university prints this message when you log in (quotation marks are in the original):

This system is for the use of authorized users only. Individuals using this computer system without authority or in the excess of their authority are subject to having all their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system or in the course of system maintenance, the activities of authorized user may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of illegal activity or violation of University regulations system personnel may provide the evidence of such monitoring to University authorities and/or law enforcement officials.

This is an interesting approach to the Fourth Amendment: pressure most everyone to agree, in advance, to waive their rights under it.

References

- The administration's “White Paper”: Information Infrastructure Task Force, Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual

Property Rights (1995).

- [An explanation of the White Paper: The Copyright Grab](#), Pamela Samuelson, Wired, Jan. 1996
- [Sold Out](#), James Boyle, New York Times, 31 March 1996
- Public Data or Private Data, Washington Post, 4 Nov 1996. We used to have a link to this, but Washinton Post has decided to start charging users who wishes to read articles on the web site and therefore we have decided to remove the link.
- [Union for the Public Domain](#)—an organization which aims to resist and reverse the overextension of copyright and patent powers.

(This copy of "The Right to Read" was obtained from <http://www.gnu.org/philosophy/right-to-read.html> on 2008-06-24.)