The SPA, which actually stands for Software Publishers Association, has been replaced in its police-like role by the Business Software Alliance. The BSA 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 in prison.

- The university security policies described above are not imaginary. For example, a computer at one Chicago-area university displayed this message upon login:

  > 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.

Bad News

The battle for the right to read is going against us so far. The enemy is organized, and we are not.

Today's commercial e-books abolish readers' traditional freedoms. Amazon's e-book reader product, which I call the "Amazon Swindle" because it's designed to swindle readers out of the traditional freedoms of readers of books, is run by software with several demonstrated Orwellian functionalities. Any one of them calls for rejecting the product completely:

- It spies on everything the user does: it reports which book the user is reading, and which page, and it reports when the user highlights text, and any notes the user enters.
- It has DRM, which is intended to block users from sharing copies.
- It has a back door with which Amazon can remotely erase any book. In 2009, it erased thousands of copies of 1984, by George Orwell.
- In case all that isn't Orwellian enough, there is a universal back door with which Amazon can remotely change the software, and introduce any other form of nastiness.

Amazon's e-book distribution is oppressive, too. It identifies the user and records what books the user obtains. It also requires users to agree to an antisocial contract that they won't share copies with others. My conscience tells me that, if I had agreed to such a contract, the lesser evil would be to defy it and share copies anyway; however, to be entirely good, I should not agree to it in the first place. Therefore, I refuse to agree to such contracts, whether for software, for e-books, for music, or for anything else.

If we want to stop the bad news and create some good news, we need to organize and fight. Subscribe to the FSF's Defective by Design campaign to lend a hand. You can join the FSF to support our work more generally. There is also a list of ways to participate in our work.

The Right to Read - GNU Project

by Richard Stallman

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

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. (Ten percent 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 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.

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 Notes

- This story is supposedly a historical article that will be written in the future by someone else, describing Dan Halbert's youth under a repressive society shaped by the unjust forces that use “pirate” as propaganda. So it uses the terminology of that society. I have tried to project it forwards into something more visibly oppressive. See “Piracy”.

- Computer-enforced restrictions on lending or reading books (and other kinds of published works) are known as DRM, short for “Digital Restrictions Management”. To eliminate DRM, the Free Software Foundation has established the Defective by Design campaign. We ask for your support.

  The Electronic Frontier Foundation, a separate organization not related to the Free Software Foundation, also campaigns against DRM.

- The battle for the right to read is already being fought. Although it may take 50 years for our past freedoms to fade into obscurity, most of the specific repressive laws and practices described above have already been proposed; some have been enacted into

law in the US and elsewhere. In the US, the 1998 Digital Millennium Copyright Act (DMCA) gave explicit government backing to the computer-enforced restrictions known as DRM, by making the distribution of programs that can break DRM a crime. The European Union imposed similar restrictions in a 2001 copyright directive, in a form not quite as strong.

The US campaigns to impose such rules on the rest of the world through so-called “free trade” treaties. Business-supremacy treaties is a more fitting term for them, since they are designed to give business dominion over nominally democratic states. The DMCA's policy of criminalizing programs that break DRM is one of many unjust policies that these treaties impose across a wide range of fields.

The US has imposed DMCA requirements on Australia, Panama, Colombia and South Korea through bilateral agreements, and on countries such as Costa Rica through another treaty, CAFTA. Obama has escalated the campaign with two new proposed treaties, the TPP and the TTIP. The TPP would impose the DMCA, along with many other wrongs, on 12 countries on the Pacific Ocean. The TTIP would impose similar strictures on Europe. All these treaties must be defeated, or abolished.

Even the World Wide Web Consortium has fallen under the shadow of the copyright industry; it is on the verge of approving a DRM system as an official part of the web specifications.

- Nonfree software tends to have abusive features of many kinds, which lead to the conclusion that you can never trust a nonfree program. We must insist on free (libre) software only, and reject nonfree programs.

  With Windows Vista, Microsoft admitted it had built in a back door: Microsoft can use it to forcibly install software “upgrades,” even if users consider them rather to be downgrades. It can also order all machines running Vista to refuse to run a certain device driver. The main purpose of Vista's clampdown on users was to impose DRM that users can't overcome. Of course, Windows 10 is no better.

- 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 gave early versions names such as “trusted computing” and “Palladium”, but as ultimately put into use, it is called “secure boot”.

  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 per own computer. Microsoft is likely to use that control on behalf of the FBI when asked: it already shows the NSA security bugs in Windows to exploit.

  Secure boot can be implemented in a way that permits the user to specify the signature key and decide what software to sign. In practice, PCs designed for Windows 10 carry only Microsoft's key, and whether the machine's owner can install any other system (such as GNU/Linux) is under Microsoft's control. We call this *restricted boot*.

- In 1997, when this story was first published, the SPA was threatening small Internet service providers, demanding they permit the SPA to monitor all users. Most ISPs surrendered when threatened, because they could not afford to fight back in court. One ISP, Community ConneXion in Oakland, California, refused the demand and was actually sued. The SPA later dropped the suit, but the DMCA gave it the power it sought.