Richard Stallman

THE RIGHT TO READ

societal dimensions

(from "The Road To Tycho," a collection of articles about the antecedents of the Lunarian Revolution, published in Luna City in 2097)

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 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 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 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

> “Computers can be used as tools or weapons. I don’t want to see computers used the wrong way, to hurt people.”
>
> —Manuel Braga, age 16, New York City

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 Internet. 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; 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

http://www.horizonsmedia.com/csuri

“I Become What I Think” Charles Csuri, 1995.

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 U.S. 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

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 in this essay have already been proposed—either by the Clinton administration or by publishers.

There is one exception: the idea that the FBI and Microsoft will keep the root passwords for personal computers. This is an extrapolation from the Clipper chip and similar Clinton administration key-escrow proposals, together with a long-term trend: computer systems are increasingly set up to give absentee operators control over the people actually using the computer system.

The SPA, which actually stands for Software Publisher's Association, is not today an official police force. Unofficially, it acts like one. It invites people to inform on their coworkers and friends; like the Clinton administration, it advocates a policy of collective responsibility whereby computer owners must actively enforce copyright or be punished.

The SPA is currently threatening small Internet service providers, demanding they permit the SPA to monitor all users. Most ISPs surrender when threatened, because they cannot afford to fight back in court (*Atlanta Journal-Constitution* Oct. 1, 1996, D3). At least one ISP, Community ConneXion in Oakland CA, refused the demand and has actually been sued (http://www.c2.net/ispdc/). The SPA is said to have dropped this suit recently, but they are sure to continue the campaign in various other ways.

The university security policies described here are not imaginary. For example, a computer at one Chicago-area university prints this message when a user logs 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 users 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 and Notes

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 (http://www.hotwired.com/wired4.01/ features/ whitepaper.html).

Sold Out. James Boyle, *New York Times*, 31 March 1996 (http:// www.ese.ogi.edu/sold.out.html).

Public Data or Private Data. *Washington Post*, 4 Nov 1996 (http:// wp2.washingtonpost.com/

Union for the Public Domain—a new organization that aims to resist and reverse the overextension of intellectual property powers. For more information, see http://www.public-domain.org/.

Richard Stallman (rms@ai.mit.edu) received the 1990 ACM Grace Murray Hopper award for developing GNU Emacs. He is also the author of the free symbolic debugger GDB, and founded the project to develop the free GNU operating system.