

# YOU

bought it.

**A LEADING THINKER ON THE IRONIES OF TECHNOLOGY ARGUES THAT MACHINES MEANT TO LIBERATE US ARE INSTEAD PUTTING CONSUMERS IN A STRAITJACKET—AND STIFLING VITAL INNOVATION IN THE PROCESS. ESSAY BY EDWARD TENNER • ILLUSTRATIONS BY STUART BRADFORD**

# WHO

controls it?

**T**he personal-computing revolution began with a promise: after decades of submission to centralized mainframes, ordinary users were now in control. Buttoned-up IBM loosened its collar, opened its new PC to accommodate hardware and software from a variety of suppliers, and even bought its operating system from a couple of Harvard University dropouts. To reinforce this message, IBM chose as its marketing emblem a look-alike of Charlie Chaplin—timeless hero of the harried underdog. It was a clever choice, and not inappropriate: the PC and other machines like it really did confer upon users a degree of control over information never before available. Twenty years later, technology industries are still promising us autonomy and independence.

But that promise is falling flat. Asserting an unprecedented degree of control over their goods, even once they are in the customers' hands, technology producers are moving to circumscribe the freedom that technology users have long taken for granted. The same powerful trends that have brought leaps in performance—ubiquitous microprocessors, cheap digital storage, and virtually free data transmission—are making possible new ways for technology makers to control users' behavior. These developments reek more of Big Brother than the Little Tramp.

It's not that companies have ill intent. Manufacturers are offering hardware and code they claim will release the full potential of information technology: promoting creativity and productivity while making computing and the Internet secure and reliable at last. Their products address real problems—from brand counterfeiting and piracy, which cost billions, to malfunctioning equipment. But despite the benign intent, some features built into new generations of devices, like the Greek infiltrators in the belly of the Trojan horse, provide openings for intrusion and even conquest. Call it the Trojan mouse.

as the distinction between home and office blurs, consumers now find themselves wrestling with the sort of constraints once intended mainly for corporate users. Microsoft is leading the way by beginning to license its Windows operating system for household use in much the way it deals with businesses: each machine must have its own paid upgrade to the next version. Users do have the right to continue running older versions of Windows, but they may find that new programs they want or need run only on the latest release. The result is “forced migration,” to use a stark metaphor dating from the mainframe era. Other technology and entertainment companies are also cracking down through incapacitation. Instead of paying more patent and copyright lawyers to take alleged infringers to court, they are modifying their products so that the user is physically barred from using them in unsanctioned ways. The traffic cop is giving way to the speed bump.

## Information Lockdown

**I**n the early days of the PC software industry, elaborate anti-copying systems blocked users from duplicating programs for use by friends or colleagues. By the 1990s, consumer resistance had restricted copy protection to niche products such as computer-assisted-design programs. But now, companies are reimposing such limits. Here again, technology producers are displaying a taste for incapacitation.

Yes, copyright owners have tried using accountability—they took Napster to court and brought the file-sharing service down with a lawsuit. But that was a victory in one battle of what has become a widening war; a new file-sharing network seems to rise from the ashes of each defeated one. Individual songs and entire movies are now routinely available on the Web weeks before their official release. While the music industry is beginning to introduce its own download sites online and, soon, in retail stores, it is also alarmed by peer-to-peer exchange among friends. Soon, even entry level personal computers will have the

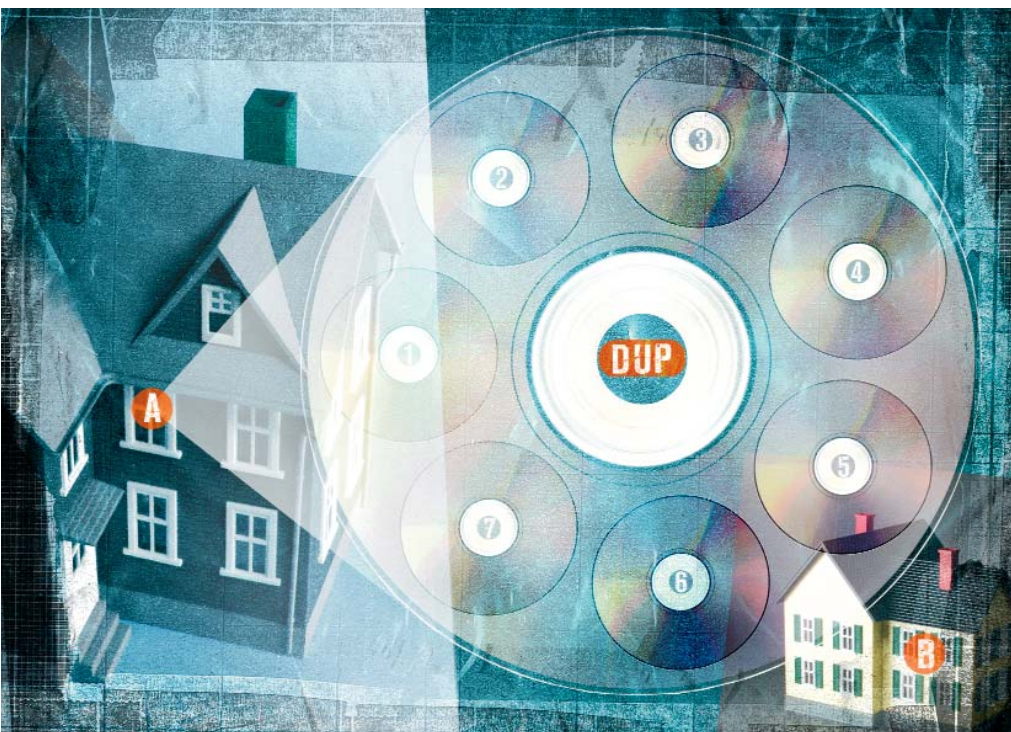
**MEASURES TO CONTROL BEHAVIOR CAN DEPEND EITHER ON ACCOUNTABILITY (THINK TRAFFIC COPS) OR INCAPACITATION (SPEED BUMPS). MAKERS OF TECHNOLOGY ARE TURNING MORE AND MORE TO THE STRATEGY OF INCAPACITATION.**

Measures to control behavior can depend on either accountability or incapacitation. Think of automotive traffic control. Until recently, most communities tried to control speeding with radar-equipped patrol cars. More recently, some towns have shifted to a strategy of incapacitation: they are making speeding physically difficult with increasing use of “traffic-calming” devices such as speed bumps. Police radar is a technology of accountability; it needs the courts to be effective and can be defeated at least some of the time by sensitive detectors. Traffic-calming structures, by contrast, are technologies of incapacitation: they limit passively what people can do with their vehicles.

Technology makers increasingly prefer incapacitation as a strategy of control. The software industry, for example, once used a double standard for enforcing its licenses: companies vigorously regulated software usage by commercial establishments while pretty much letting individual consumers do as they pleased. But

capability to record CDs and DVDs, and enough disk space for hours of music and video. The consumer, in other words, is becoming a low-cost rival manufacturer and, through Internet file sharing, an essentially zero-cost rival distributor. The strategy of accountability, it seems, is losing the war.

Companies have already begun to limit movements of data. Sony, a leading audio and video company and copyright owner, may be offering a preview of controls to come. Some of its computers already use proprietary software to encrypt digital music, limiting the number of times a song can be downloaded (“checked out,” in Sony’s parlance) to an external device. After three downloads, a song must be “checked in” to the original device before it can be checked out again. While the aim is protection of copyrighted material, the program makes it difficult to duplicate any CD at all—including one that contains music created and recorded by the owner.



Such schemes will of course have little effect against the greatest economic threats to the copyright holders: the pirate factories of eastern Europe and Asia. These illicit operations can pay technical experts to defeat protection, or bribe insiders for unprotected copies of source material. Whether intentionally or not, therefore, Sony is targeting the controls at the less serious losses from sharing among friends.

Why should a legitimate owner of a CD or DVD object to such copy protection? These schemes do, after all, permit backups and second copies for use in other machines, such as portable or automobile CD players. But the controls can also degrade the quality of the product. Even some electrical engineers who believe that sophisticated copy protection is undetectable to most listeners acknowledge that because music and videos already make use of data compression algorithms that take advantage of the limits of human senses, a few people with especially discerning ears may indeed be able to tell the difference. Moreover, copy control often works by weakening the error correction schemes in the stored data—an alteration that may wash out subtleties of performance or make discs less scratch resistant.

Last October, *Audio Revolution* magazine reported that DVD players constructed without the normally mandated series of internal conversions between digital and analog formats—circuits included by industry agreement purely to foil piracy—produce “stunning” images compared to those from conventional players. The British organization Campaign for Digital Rights has denounced copy protection as an unacceptably blunt weapon against piracy: determined outlaws can still find computers that will allow the CDs to be ripped for MP3s, while honest consumers receive what many audio and video enthusiasts consider musically compromised products.

Despite the complaints, past experience has shown that what technology *can* control, the law *will* control—or at least try to. That’s exactly what has happened here, as constraints on data copying draw strength and legitimacy from the force of the Digi-

tal Millennium Copyright Act of 1998. This legislation provides harsh penalties not only for piracy but also for publicizing ways to circumvent security. So far, however, the law appears not to have slowed the diffusion of control-evading techniques: the anarchical impulse of technology users is not easily suppressed.

## Security vs. Freedom

In the most thorough form of incapacitation, technology makers are building their products to resist any form of alteration once they leave the factory. The paradox here is that while many technology users resent such control, they also need it. A computer network that is truly open, for example, is also dangerously vulnerable to attack by viruses.

Not surprisingly, these days the computer industry is giving higher priority to security than openness. Take, for example, the controversial Microsoft project origi-

nally known as Palladium and recently renamed Next-Generation Secure Computing Base for Windows. This effort involves the development of a set of secure features for a new generation of computers. The goal: let users such as banks communicate in ways that prevent disclosure of information to unauthorized persons, using stronger hardware as well as software protection. The system would protect the privacy of medical and financial data far more effectively than today’s security software, and Microsoft insists that it will not restrict the rights of most computer owners; machines will be shipped with the new capabilities turned off.

A computer built on the new specification could run existing software like any other. But the Secure Computing Base could give Microsoft or other vendors the power to disable third-party software on their customers’ computers, if they believe it circumvents rights management. Vendors could also detect and disable user hardware modifications that, as judge, jury, and executioner, they deem a threat to the security of their programs. As evidence of this intent, critics point to phrases in the user license agreements of Microsoft’s Windows Media Player that seem to allow the program’s security updates to disable other programs. “The keys will be kept in tamper-resistant hardware rather than being hidden in software,” contends Ross Anderson, a University of Cambridge computer scientist. “There will be lots of bugs and workarounds that people discover, but eventually they will get fixed up, and it will be progressively harder to break.”

Paul England, a software architect at Microsoft familiar with the system, considers such fears unwarranted. There is, he says, “no a priori remote control” that it will impose or let others impose on a user’s applications. Copyright owners would not, he insists, be able to use the system to inactivate other programs that could capture their data and store it in different file formats.

This blanket of security can smother as well as protect. Web businesses and software vendors will have the option of offering their products only to “trusted” machines—that is, those in which the protection system has been activated. Most content

companies would probably begin to restrict compatibility to trusted machines. Downloading a magazine article or a song, for example, might require a machine in which the Microsoft technology was present and activated.

Such measures can prevent hackers and unethical companies from stealing personal information and hijacking personal machines for nefarious purposes. But tamperproofing technology also allows companies, while flying the banner of fighting piracy, to take steps that degrade the performance that law-abiding consumers get from their computers.

Critics argue that Microsoft's Secure Computing Base comes at too high a price. Princeton computer scientist Edward W. Felten warns that if technology vendors "exploit Palladium fully to restrict access to copyrighted works, education and research will suffer." Scientists, he points out, must be able to inspect and modify electronic technology, just as automotive engineers and designers must be able to take vehicles apart and tweak components.

## THE TAMPERPROOFING THAT SOME TECHNOLOGY COMPANIES ARE NOW PUTTING IN PLACE THREATENS A TRADITION OF USER-CENTERED INNOVATION. INCAPACITATING DESIGNS WILL SLAM THE DOOR ON THESE VITAL SUPERTINKERERS.

Indeed, the kinds of tamperproofing now being put in place threaten the individual tinkering upon which so much innovation is based. They would deprive people of their long-standing right to improve on products they lawfully own—even when they are not violating copyrights or creating hazards. Such user-centered innovation has a long history in the United States. Henry Ford's Model T and tractor, for example, were made for resourceful country people who constantly found new uses for them: once the drive axle was lifted and a wheel removed, the hub could drive tools and farm equipment. It was a mini power station on wheels, its variations and applications limited only by the user's imagination.

Some contend that the freedom users have to modify a system and its software is worth the risk. As John Gilmore, a cofounder of the Electronic Frontier Foundation, a Washington, DC-based civil-liberties organization, has written, "Be very glad that your PC is insecure—it means that after you buy it, you can break into it and install what software you want. What *you* want, not what Sony or Warner or AOL wants."

### The Cost of Control

Legislation now pending would make tamperproofing the law of the land. Senator Fritz Hollings (D-South Carolina) has introduced a bill that would require all electronic devices—from computers to Furby toys—to have built into them some form of rights-management or security software that would limit users' rights to inspect and modify them. According to Hollings's office, the measure is intended to prod the electronics and media industries to come to an agreement on security standards.

Some information technology experts remain sanguine. Even if the Hollings bill becomes law, they contend, competition and market pressures will preserve people's freedom to modify the technological products they buy. Mark Granovetter,

a professor of sociology at Stanford University, says that a massive public backlash would prevent Microsoft from implementing the Secure Computing Base.

Others, however, are more pessimistic. Jonathan Zittrain, a professor of information law at Harvard, foresees the introduction of "closed, appliance-like devices as substitutes for the general PC." Such appliances would be more reliable than PCs but would offer their owners less control. Zittrain fears the end of what will be seen, in retrospect, as a fleeting era of computer freedom. "A diverse and vibrant community of independent software developers and vendors," he says, may have been "a transitory phenomenon of the 1980s and 1990s."

If Zittrain's prophecy proves correct, the locked-down landscape of technology will disappoint its architects. First, incapacitation will not eliminate the costs of accountability but rather shift them. A regime of constraints depends on laws banning technologies that would defeat or circumvent the control schemes, and

those bans will need to be enforced. Second, protection may degrade data, if only subtly, and introduce bugs that may stain a brand's reputation and compromise its market share.

Most seriously, forms of control that work through incapacitation will undermine the chaotic, dynamic society that made the personal-computing revolution possible in the first place. Powerless against determined pirates, they would strike hardest at creative customers, such as the chip-modifying fans who have breathed new life into moribund computer games—the very people whose ideas could help develop new generations of lucrative products. As MIT management professor Eric von Hippel wrote in 2001 in the *Sloan Management Review*, "innovations that only a few leaders use today may be in general demand tomorrow"—especially, he says, if early adopters "have a chance to innovate, to learn by doing, and to develop the general utility of their innovations." Incapacitating designs will slam the door in the faces of these vital supertinkerers.

Incapacitation would also limit the academic training of companies' future technical staff. Freedom to tinker—defined by Felten as "your freedom to understand, discuss, repair, and modify the technological devices that you own"—benefits technology industries most of all. Even the film industry needs young people who have had free access to the nuts and bolts of digital graphics and special effects, and I'll bet that Microsoft doesn't make its young Xbox game-programming recruits sign an affidavit that they have never violated an end-user license agreement. New hardware security is manifestly a good idea for servers with sensitive information. There is a good case for new levels of protection, like the Microsoft scheme, for these vulnerable sites. But if they extend incapacitation too far, the builders of the Trojan mouse may find themselves caught in their own trap. ■

---

*Edward Tenner is author of Why Things Bite Back: Technology and the Revenge of Unintended Consequences and the forthcoming Our Own Devices: The Past and Future of Body Technology (Knopf).*

