

CODIFICATION

Anti-trusting Microsoft

The software giant looking to gain our trust with Palladium.

By Lawrence Lessig
September 10, 2002

Imagine a Monty Python skit with John Cleese riding on a bus. Out of the blue, he hits the person standing to his left. Stunned, the person says, "You just hit me."

"No I didn't," Mr. Cleese responds. A few seconds later, Mr. Cleese hits the person standing to his right.

"Hey, you hit me," that person says.

"No I didn't," Mr. Cleese insists. A few seconds later, Mr. Cleese hits again. Again, he's accused. Again, he denies. Soon, Mr. Cleese can't move a muscle without everyone around him cowering. He stands to give someone his seat; the person jumps back. He reaches out to help an old lady, and passengers scream.

Microsoft has a John Cleese problem. Again and again, it has been accused of anticompetitive behavior. Again and again, it has denied it. When the Clinton administration sued it, the company insisted it was "totally innocent." When a unanimous court found it guilty, its chairman took to the airwaves to declare victory. Not once have the leaders or lawyers openly acknowledged they were wrong. Thus, quite understandably, the world trembles every time Microsoft moves.

This is too bad, and not just for Microsoft. I've long criticized the company's failure to talk straight about the law, and I certainly believe we shouldn't trust that Microsoft understands what it cannot explain. But there are more issues out there than whether Microsoft will hit again. And by obsessing on this one problem, we miss the ways Microsoft could help solve others.

The fury about Microsoft's June announcement of Palladium is a perfect example. Named after the mythical statue that guarded Troy, Palladium implements a "trusted computing architecture" on the Windows platform. If this crucial bit of the operating system works as designed, a Palladium-enabled machine could give users interacting with it assurance that the machine will do just what it says. If you sent a Palladium-equipped machine an email, but told it not to forward the email, the machine would obey the restriction. If Disney sent a movie, and said, "play this only three times," the machine would obey that restriction, too. A trusted architecture would make it easier for users interacting with trusted machines to control how those machines use their content. And for anyone who's had an email turn up somewhere it shouldn't, this type of control doesn't sound all bad.

Microsoft has thus sold Palladium in the name of privacy and security. But commentators have quickly skipped over these parts, focusing instead on whether Palladium would enable Microsoft to hit again. The technology, these commentators argue, will give Microsoft more control over competition; it could shut out open-source software and content not made for Windows. Palladium is therefore no guard, these commentators insist. Palladium is a Trojan horse.

These are valid concerns, but they obscure something important about how trusted platforms could change the debate about digital rights management (DRM). For, by increasing trust at the ends of the network, Palladium would weaken an argument that Hollywood now pushes: that Congress regulate every machine on the Internet to protect Hollywood's content. Trusted platforms could enable a different kind of DRM--indeed, I would say, a "better DRM"--one less damaging to innovation and more supportive of content competition.

To see the point, distinguish between DRM systems that control copying (copy-protection systems) and DRM systems that control who can do what with a particular copy ("token" systems that Palladium would enable). Copy-protection systems regulate whether machine X can copy content Y. Token systems regulate whether, and how, machine X is allowed to use content Y.

The difference can be critical to network design: if a technology could control who used what content, there would be little need to control how many copies of that content lived on the Internet. Peer-to-peer systems, for example, depend upon many copies of the same content living in many different places across the Net. Copy-protection systems defeat this design; token systems that respect the network's end-to-end design need not.

No doubt "better DRM" raises hard policy questions. Would token systems on their own adequately protect "fair use"? (Probably not.) Is "better DRM" preferable to no DRM at all? (Certainly not.)

But these questions are distinct from the antitrust questions that hound Microsoft. They are obscured as long as the world jumps whenever Microsoft moves. Yet so long as Microsoft lives by denial, it will be known only by what it denies--regardless of any good built into its designs.

Lawrence Lessig is a professor of law at Stanford Law School. Write to letters@redherring.com.

Write to [Laurence Lessig](mailto:Laurence.Lessig).

Gainers

Millennium Pharm	7.41	5.86%
Advanced Micro Devices	5.53	5.33%
Tpsa Telekom Polska	3.03	4.92%

Decliners

Silverline Technologies	0.19	-13.24%
Orascom Telecom Holding	2.42	-12.02%
Net One Systems Co	3765.17	-10.31%