

From: Larry Blunk
To: Microsoft ATR
Date: 1/28/02 5:16pm
Subject: Microsoft Settlement

I wish to stress my opposition to current United States vs. Microsoft proposed Settlement Agreement. The numerous loopholes and lack of consequences for violation of the agreement will result in little or no change in Microsoft's anti-competitive behaviour.

Perhaps most unsettling is the area of DRM and authentication systems, and audio/video codecs. Microsoft is attempting and dominate these fields through it's .Net and Windows Media services initiatives. There is no mention at all of compulsory licensing of audio/video codecs in the settlement. If Microsoft is able to monopolize these standards, they will extend their control beyond just PC hardware OEM's to all manner of audio/video playback devices. These include pocket audio players, personal video recorders, component audio receivers, DVD players, and handheld organizer (such as the Palm Organizer). All these device makers and will need to license the audio/video codecs on Microsoft's terms. These terms will likely forbid the use of competitive operating systems such as Palm OS and Linux on these devices. It will also require the use of Windows backend server operating systems rather than competing operating systems such as Unix.

Closely related to the audio/video codecs are Microsoft DRM systems which are used to wrap and "secure" the codecs. DRM services are specifically excluded from compulsory licensing. The rationale is that licensing them would somehow undermine their effectiveness. However, there is no reason these systems could not be licensed under a standard non-disclosure agreement (NDA). The same type of agreement could be used for authentication systems. I also note that there is a major flaw in the Department's understanding of authentication and cryptographic systems. A basic tenet in cryptography is that in order to be trusted, a cryptographic system should be subjected to extensive public peer review. Rather than relying on secrecy for security, authentication systems rely on the strength of their cryptographic algorithms. Even though the algorithms are widely published, they remain secure because of the mathematical complexities in defeating them. It should be noted that the standard for securing transactions on the Web today (such as credit card purchases) is the openly specified SSL standard. SSL employs only publicly documented and reviewed cryptographic mechanisms. There is even an open source implementation known as OpenSSL which is used extensively to secure transactions on the Internet. This is a difficult concept for the layman to understand, but it is critical to an open and competitive environment on the Internet.

-Larry J. Blunk
Saline, Michigan USA

Do You Yahoo!?
Great stuff seeking new owners in Yahoo! Auctions!
<http://auctions.yahoo.com>