Filters Get Clogged:
Legal and Technical Problems for Internet Filtering (1)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

A couple of items lately caught my eye concerning Internet content filtering software (a.k.a. "censorware").   I was first made aware of the issues through journalist Declan McCullagh's excellent POLITECH mailing list <http://www.politechbot.com/info/subscribe.html >.

The first item is that in mid-December, without much public fanfare, Congress passed the Children's Internet Protection Act (CIPA) and the Neighborhood Internet Protection Act (NIPA), and President Clinton signed them into law (Public Law 106-554).   These laws, effective as of April 20, 2001, penalize any libraries that don't use blocking or filtering software ("censorware"); the penalty will consist of elimination of discounts (the "E-rate") currently provided under the Library Services and Technology Act, Title III of the Elementary and Secondary Education Act and the Universal Service discount program.   For full details of the CIPA see the American Library Association's CIPA Web page at < http://www.ala.org/cipa/>.

On January 18th, the ALA announced that the Association will launch legal action challenging the constitutionality of the CIPA.   Their press release included the strong statement, "No filtering software successfully differentiates constitutionally protected speech from illegal speech on the Internet. Even the federal commission appointed to study child safety on the Internet concluded filters are not effective in blocking all content that some may find objectionable, but they do block much useful and constitutionally protected information."

The second item popped up in FindLaw's DOWNLOAD THIS! ("A Weekly Newsletter Covering Law and the Internet") Issue # 18< http://my.findlaw.com > for January 19, 2001.   The abstract explained that users of Microsoft's Hotmail service have been unable to send e-mail to the anti-censorware group Peacefire <http://www.peacefire.org >for the last five months (see < http://news.cnet.com/news/0-1005-201-4523924-0.html > and for details).   Seems Hotmail silently trashed outgoing e-mail to Peacefire because that organization happens to be hosted by an ISP on the Realtime Blackhole List <http://mail-abuse.org/rbl+/ >, a project of the Mail Abuse Prevention System (MAPS) to automate exclusion of Internet communications with violators of its anti-spam guidelines.   The critical issue is that Hotmail did not tell its users the truth about the discarded e-mail: according to Bennett Haselton, writing in RISKS <http://catless.ncl.ac.uk/Risks/21.22.html#subj9 >, "If you tried to send mail to a peacefire.org address from HotMail, you'd get a fake error message a day later saying that there was a problem on the recipient's end -- when it was really HotMail blocking the message from being delivered."   This block has been listed for Peacefire's ISP, but it remains in effect for many other blocked sites.   You would think that simple honesty (if courtesy is beyond reach) would make Hotmail staff explain the problem truthfully.

In the next part of this article I will look at how these two items are fundamentally related.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>.   He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and

his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.