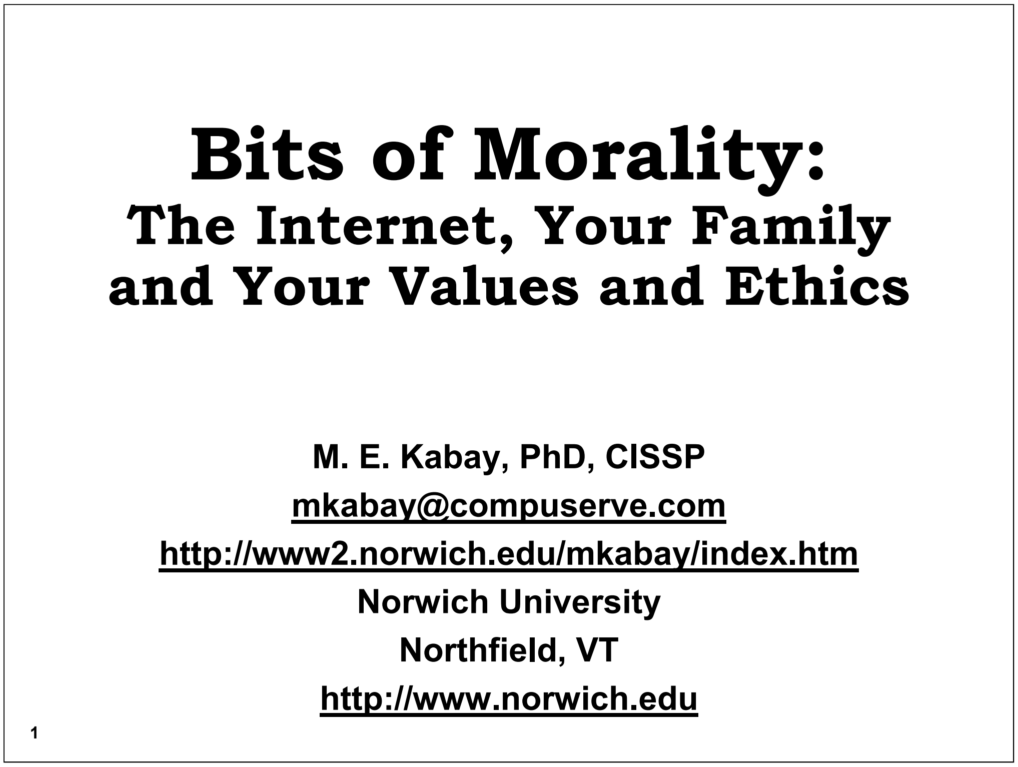


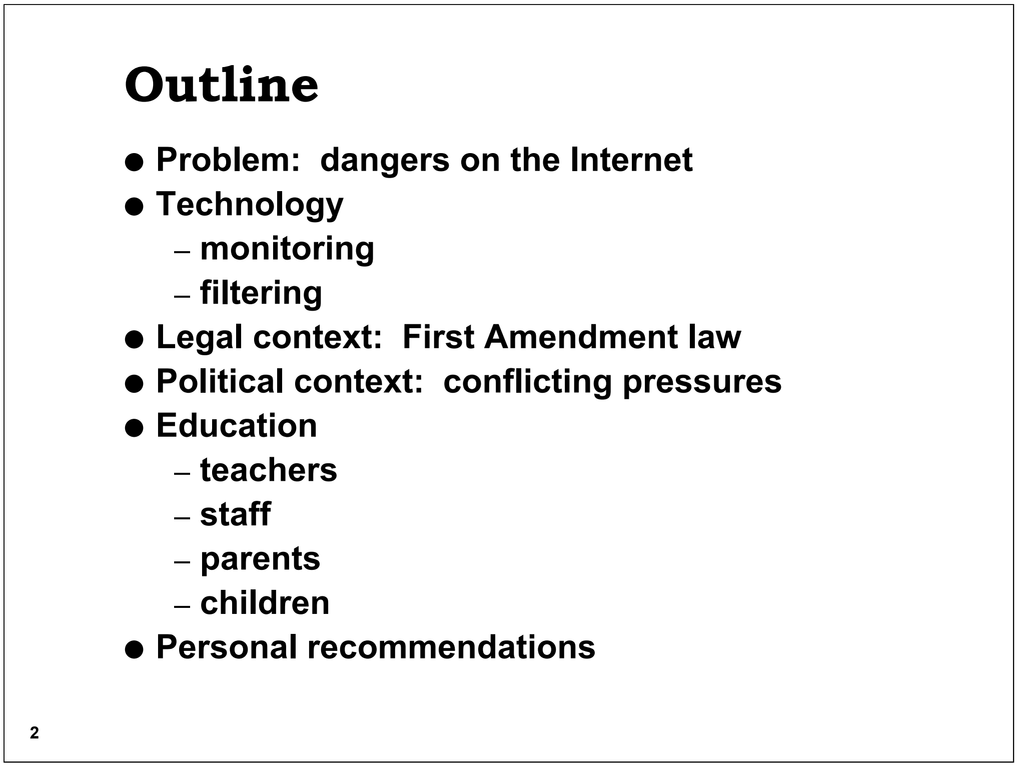
Bits of Morality:
The Internet, Your Family and Your Values and Ethics

M. E. Kabay, PhD, CISSP
mkabay@compuserve.com
http://www2.norwich.edu/mkabay/index.htm
Norwich University
Northfield, VT
http://www.norwich.edu

1

Norwich University
Northfield, VT
http://www.norwich.edu

M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield, VT
255 Flood Road
Barre, VT 05641-4060
V: 802-479-7937
E: mkabay@compuserve.com



Outline

- Problem: dangers on the Internet
- Technology
  - monitoring
  - filtering
- Legal context: First Amendment law
- Political context: conflicting pressures
- Education
  - teachers
  - staff
  - parents
  - children
- Personal recommendations

2

1. The following URLs have valuable background information for parents, educators and others interested in looking at morality in cyberspace:

ACLU Cyberliberties News: http://www.aclu.org/issues/cyber/hmcl.html

Center for Democracy and Technology: http://www.cdt.org

CyberCitizen Partnership: http://www.cybercitizenpartners.org/

Electronic Frontier Foundation: http://www.eff.org/

Electronic Privacy Information Center: http://www.epic.org/

Ethics and Information Technology (Journal): http://www.wkap.nl/journals/ethics_it

NetParents: http://www.netparents.org/

Parent's Guide to Internet Safety: http://www.fbi.gov/library/pguide/pguide.htm

Politech Archives: http://www.politechbot.com/

Web-Wise Kids: http://www.webwisekids.com/

ZDNet Destination Unknown (1997):
http://www.zdnet.com/zdnn/special/kids_online.html

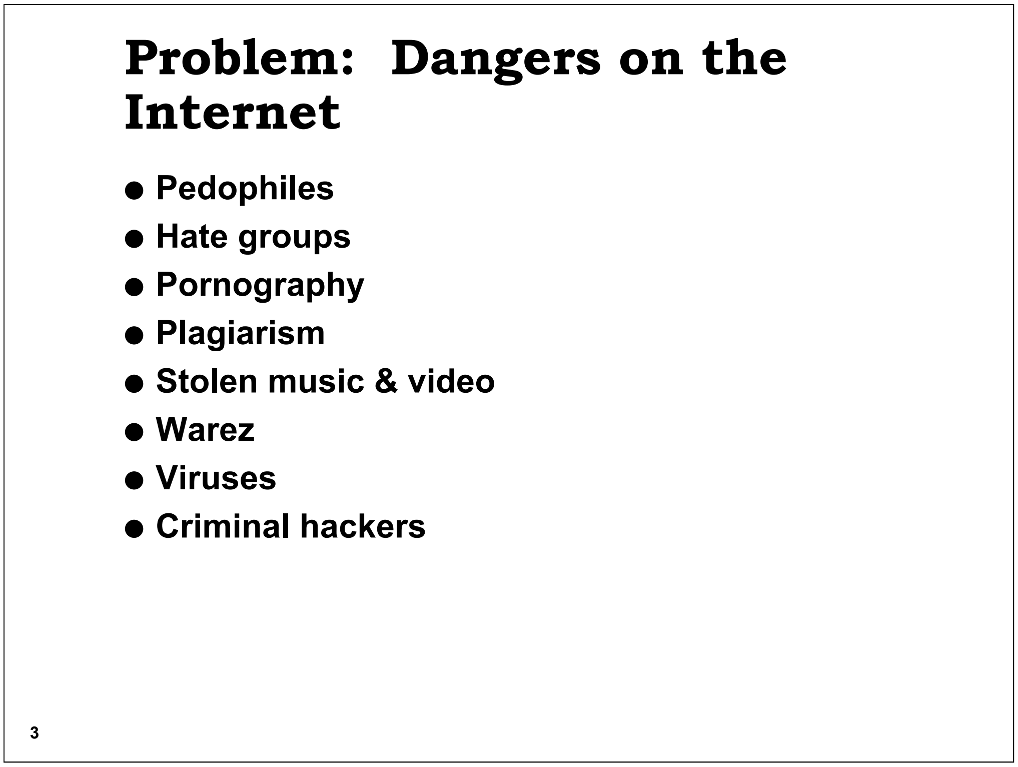
Concerning copyright – a message from M. E. Kabay, PhD, CISSP:

a. The copyrighted material incorporated into these notes remains the property of the original copyright holdres.

b. I have relied on the Fair Use doctrine when incorporating materials by other authors into these notes on the grounds that (i) this course is not for profit; (ii) there is no damage to the monetary interests of the copyright holders in printing them directly in this workbook for use by educators.

c. The slides and the assemblage of information in these lecture notes are copyright by me.

d. Do not reproduce this workbook without my explicit permission.



Problem: Dangers on the Internet

- Pedophiles
- Hate groups
- Pornography
- Plagiarism
- Stolen music & video
- Warez
- Viruses
- Criminal hackers

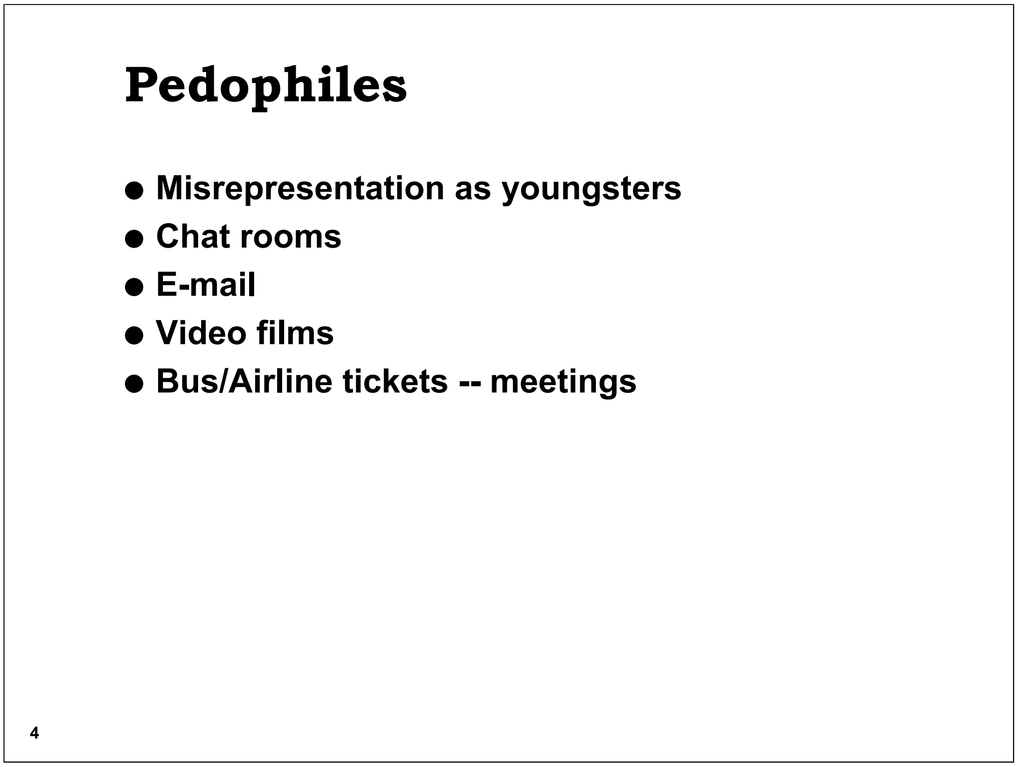
3

1. For reviews of key events across the entire field of information security, see

   Kabay, M. E. (1996-2000). *The INFOSEC Year in Review.* Available for free download (registration required) as PDF files at http://www.icsa.net/html/library/whitepapers/#infosec

2. See also the related paper

   Kabay, M. E. (2000). *Why Kids Shouldn't Be Criminal Hackers* http://securityportal.com/cover/coverstory20001009.html



Pedophiles

- Misrepresentation as youngsters
- Chat rooms
- E-mail
- Video films
- Bus/Airline tickets -- meetings

4

Kabay, M. E. (1998). *The INFOSEC Year in Review 1997.* http://www.icsa.net/html/library/whitepapers/infosec/InfoSec_Year_in_Review_1997.pdf

1997-02-12 (AP)

Paul Brown, Jr, a 47-year-old, 400-pound man, misrepresented himself as a 15 year-old boy in e-mail to a 12-year old girl in New Jersey. He was arrested in February and police found correspondence with at least ten other teenaged girls across the country. Brown convinced his young victims, some as young as 12, to perform various sexual acts in front of cameras and send him pictures and videotapes. He pleaded guilty in June to enticing a minor into making pornography. He faced fines of up to $250K and 5 years in prison. In August, one of his many victims told the court that she had suffered ridicule and humiliation as a result of her entrapment and had left her school to escape the trauma. She accused Brown of emotional rape. Displaying an astonishing interpretation of his own behavior, Brown said at his sentencing hearing, "It was just bad judgment on my part." Using good judgment, the court sentenced him to five years incarceration.

1997-04-08 (AP)

FBI Director Louis Freeh, speaking before a Senate panel, described the Bureau's attempts to protect children in cyberspace. The "Crimes Against Children" initiative includes a program in which undercover agents monitor chat lines where pedophiles have taken to impersonating children; the agents turn the tables on the victimizers and have been responsible for 91 arrests and 83 felony convictions since 1993.

1997-06-09 (UPI)

Richard Romero went to trial in June, accused of tricking a 13-year-old boy into leaving his Chicago home for a tryst in Florida. The events allegedly took place in 1996, when Romero is accused of having befriended the child through the Net by pretending to be a 15-year-old boy. The abducted boy's mother luckily found details of the meeting place after the child had left home and police were able to track the pair with the help of a taxi driver who remembered them.

Pedophiles, cont'd

1997-07-02 (UPI)

Several police operations successfully captured pedophiles after hundreds of creeps sent sexual innuendos to a virtual girl. One was caught in Concord, CA as he prepared to enter a motel armed with condoms and a bag of Nordstrom lingerie. In another sting, police captured a homosexual pedophile in Washington, DC when he attempted to meet a virtual 13-year-old boy he had attempted to seduce via chat line.

1997-07-11 (AP)

Fox Meadow School students and staff in Scarsdale, NY were shocked to find their well-liked teacher, Robert M. Nebens, charged with interstate transportation of child pornography and interstate travel with the purpose of engaging in sex with a person under 18. FBI Special Agent Anne Figueiras posed as a thirteen-year-old boy to trap the accused pedophile into arranging a meeting in Florida via the AOL online chatroom "Barely Legal: Male-for-Male." Other children may also have been abused by Nebens, according to the FBI.

Kabay, M. E. (1999). *The INFOSEC Year in Review 1998.*
http://www.icsa.net/html/library/whitepapers/infosec/InfoSec_Year_in_Review_1998.pdf

1998-06-23 (EDUPAGE)

EDUPAGE authors wrote, "The Supreme Court has let stand a lower court ruling that frees Internet service providers such as America Online from legal liability for information one subscriber circulates to millions of others. The appeals court said that federal law `plainly immunizes computer service providers like AOL from liability for information that originates with third parties.' The case is Zeran vs. America Online, 97-1488. (San Jose Mercury News 22 Jun 98)" In October, a Florida appeals court rejected the culpability of AOL in a case where a convicted sex maniac tried to sell the plaintiff's eleven-year-old son a porn video via an AOL chat room. The plaintiff described AOL as "a home shopping network for pedophiles and child pornographers."

Kabay, M. E. (2000). *The INFOSEC Year in Review 1999.*
http://www.icsa.net/html/library/whitepapers/infosec/iyir1999.pdf

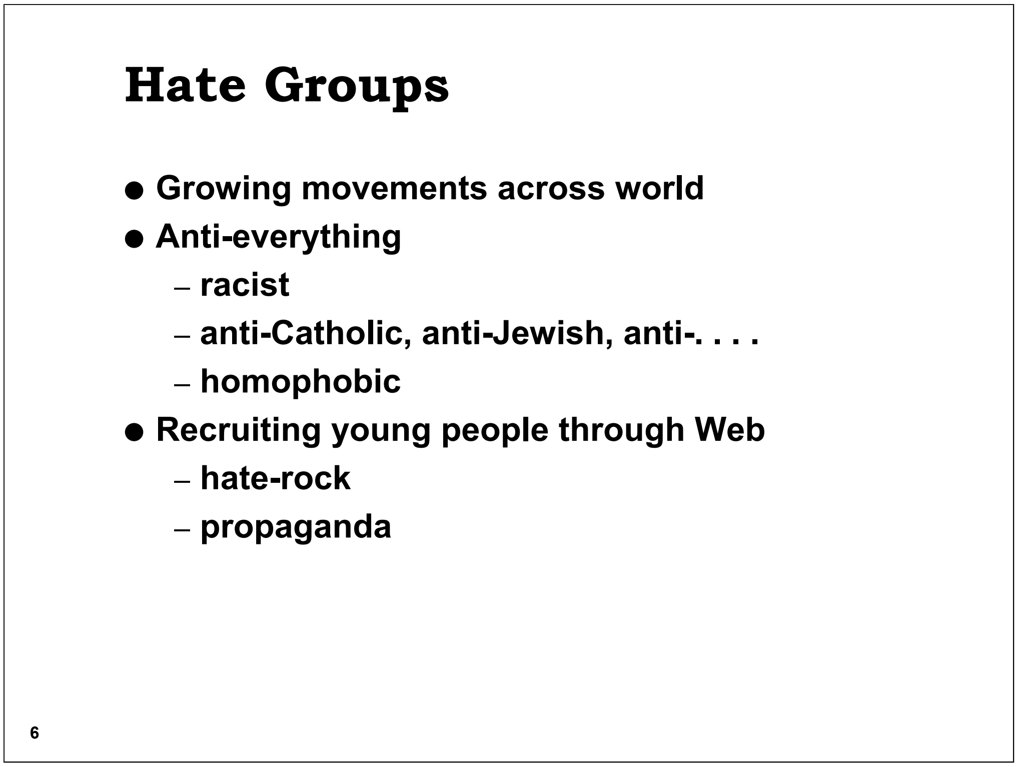
1999-01-06 (Belfast Newsletter)

Focus on Children, a Dublin-based charity, discovered a nasty nest of pedophiles operating a child-pornography exchange service on Web sites they found in mid-1996. In a 30-month investigation, the agency cooperated with the European Commission in Brussels and with police forces (including the FBI and Europol) to close in on the perpetrators.

Kabay, M. E. (2001 in press). *The INFOSEC Year in Review 2000.*

2000-08-03 (San Jose Mercury News)

Patrick Naughton, a former executive of the INFOSEEK online company, pled guilty in March 2000 to having crossed state lines to commit statutory rape of a child. Since then, said FBI officials, he has been providing help in law enforcement investigations of pedophilia on the Net. In return for his cooperation, prosecutors asked the court for five years of probation (instead of a possible 15 years in prison), counseling, a $20,000 fine (instead of the maximum $250,000) and an agreement not to have "unapproved" contact with children and to stay out of sex-chatrooms online.



Hate Groups

- **Growing movements across world**
- **Anti-everything**
  - **racist**
  - **anti-Catholic, anti-Jewish, anti-. . . .**
  - **homophobic**
- **Recruiting young people through Web**
  - **hate-rock**
  - **propaganda**

6

1. The **Southern Poverty Law Center** tracks hate groups throughout the United States. Their database of information about 457 active hate organizations is available online at http://www.splcenter.org/intelligenceproject/ip-index.html
2. **2000-01-25 (EDUPAGE).** In Britain, the Internet Watch Foundation (IWF) announced an expansion of its focus beyond the fight against child pornography. From January on, the IWF would also try to root out hate speech on the Internet. [In many countries other than the US, speech that incites hatred of or violence toward an identifiable group of people is illegal.]
3. **2000-02-18 (Inter Press Agency).** In February, an international seminar in Geneva ("Expert Seminar on Remedies Available to the Victims of Acts of Racism, Racial Discrimination, Xenophobia and Related Intolerance and on Good National Practices in this Field,") examined how national governments can fight racism without infringing on freedom of speech. Participants pointed out that censorship of hate speech is not far removed from the anti-democratic censorship practiced by totalitarian regimes worldwide. Self-regulation doesn't seem to work very well, especially with radically different levels of tolerance for expression of unpopular ideas. The conference conluded that as long as the US First Amendment protects racist and hate-spewing sites based in that country, international efforts at control are doomed.
4. **2000-07-24 (EDUPAGE).** STOPPING THE HATE ONLINE. Civil rights groups are using the Internet to fight against the bigotry of white supremacists, which were among the first groups to adopt the technology. Organizations such as the Anti-Defamation League, the Simon Wiesenthal Center, the Southern Poverty Law Center (SPLC), and smaller groups such as HateWatch, Political Research Associates, and the Center for New Community are monitoring up to 600 sites for xenophobic material, which they say is becoming more sophisticated. The work of civil rights activists involves confronting hate groups online through debate. Anti-hate groups seek to expose extremists, their half-truths, distortions, and lies through constant engagement, choosing to avoid strategies that would involve First Amendment rights. The groups forward potentially criminal information to law enforcement agencies and the SPLC has won several legal battles. The SPLC is now urging Internet service providers to act on their anti-hate policies. (Industry Standard, 24 July 2000)

Network World July 24, 2000 pNA

The trouble with regulating hate

By Keith Perine

The internet has revolutionized the business of hate. There are anywhere from hundreds to thousands of Web sites with racist or otherwise hateful content. For hate groups, the Net is a cheap and easy way to reach vast audiences under a cloak of anonymity.

"The lunatic fringe might be on the fringes, but they understand the power of the Internet as well as anyone in society," says Rabbi Abraham Cooper of the Simon Wiesenthal Center, which tracks hate groups. The center estimates there are more than 2,300 "problematic" Web sites, including more than 500 extremist sites authored by Europeans, but hosted on American servers to avoid stringent antihate laws in Europe.

HateWatch, a small East Coast group that tracks hate sites, figures there are 500 such sites on the Internet. Its research director, Brian Marcus, draws a line between methodical operations of organized groups and pages that feature racial epithets but little else. "That's not a hate site; that's graffiti on the wall," says Marcus.

While some would like to see new laws to deal with these sites - wherever they are and as many as there may be - the U.S. constitutional right to free speech protects most of them. Some European nations, however, lack the same free-speech standards. So, like other Internet policy issues such as data privacy and encryption, Europe's standards on hate speech clash with American ones. It's another instance where there's little or no consensus on how to govern this global medium.

When Timothy McVeigh bombed the Alfred P. Murrah building in Oklahoma City in 1995, perhaps the only hate site on the Web was Stormfront - a white-supremacist site run by Don Black, a former Ku Klux Klan leader who picked up some computer skills while serving a federal prison sentence in the 1980s. Stormfront has since become the grandfather of dozens of sites that espouse hatred of blacks, gays, Jews and women, deny the Holocaust and rail against abortion.

"A few years ago, a Klansman needed [to put out] substantial effort and money to produce and distribute a shoddy pamphlet that might reach a few hundred people," says Mark Potok, a spokesman for the Southern Poverty Law Center, which also monitors hate groups. "Today, with a $500 computer and negligible costs, that same Klansman can put up a slickly produced Web site with a potential audience in the millions."

Even one hate site is one too many in countries such as Germany, which has criminalized the posting of Nazi propaganda and related materials. The German constitution, written in the aftermath of the Third Reich, contains weaker speech protections than the United States' First Amendment. Moreover, German authorities are zealous about combating more than just neo-Nazism online.

In 1995, Bavarian prosecutors raided the offices of CompuServe's German subsidiary, charging the company with failing to block access to child-pornography sites. The head of the subsidiary was convicted and fined in 1998, though the conviction was reversed on appeal after the company argued that it couldn't totally block access. That key point demonstrates how the Internet's fluidity defies national norms.

And the strict German stance against objectionable content isn't going away. The Wiesenthal Center sponsored a conference last month in Berlin, where German government officials called for a set of international rules to govern online speech. The European Commission is already studying how to develop such standards, but it's not likely it will get the international cooperation it seeks, especially from the U.S.

American companies so far have been willing to make small concessions. For example, Amazon.com agreed to stop selling copies of Mein Kampf to German readers after the German government objected. But the European drive to bar online Web content hasn't put a dent in the First Amendment protections those sites enjoy in the United States - nor is it likely to do so, given the American legal tradition of protecting even the most extreme ideas.

(Cont'd on next page)

To make matters worse, hate is branching out into e-commerce, with some sites selling music, clothing, jewelry and literature. The White Heritage Emporium sells jewelry, including a swastika "Good Fortune" pendant, T-shirts and Confederate flags.

And while many ISPs refuse to host hate sites, Black sees a market opportunity: He now sells Web hosting services through Stormfront. Nazi regalia, such as daggers, uniforms and photographs, is regularly auctioned on eBay and Yahoo. Indeed, Yahoo has been sued in France, which has a law against exhibiting or selling objects that represent racism. Yahoo France filters out such objects, but the company has defied a court order instructing it to block French Web surfers from accessing the auctions through the portal's other sites. Its lawyers are expected to tell the French court that it's impractical for an Internet company to globally comply with the laws and standards of hundreds of different countries.

And that's the heart of the dilemma. National laws used to be buttressed by geographic barriers, customs inspectors and the like. But innovation has been eroding national barriers for decades, and the Internet has eroded them even further. There's no easy solution to prevent content, from the mundane to the shocking, from reaching every Internet surfer, regardless of geography. German xenophobes, for example, can easily have their Web sites hosted from the States, which in turn can be accessed from anyplace.

"If you want the Internet to come into your country, you're going to have to live with some of its openness," says Jerry Berman, executive director of the Center for Democracy and Technology, a Washington think tank. "You can't bureaucratize it."

For now, Europe hopes to make do with a filtering system being developed by the Internet Content Rating Association, a nonprofit British group that's partnered with AOL Europe and the Bertelsmann Foundation, among others. But ICRA's system hinges on the voluntary adoption of a ratings system by content providers. It's hard to imagine hate sites agreeing to rate themselves.

Yahoo's involvement with online hate doesn't end with its auction site. The company hosts dozens of online chat "clubs" devoted to neo-Nazism and other such causes, despite a clause in its user agreement that forbids "hateful or racially, ethnically or otherwise objectionable" content. Yahoo spokesman Mark Hull says the company investigates complaints and deletes grossly objectionable clubs. But it's done case by case.

"We're trying to promote inclusiveness and a wider range of free expression," adds Hull. He points out that not all chat clubs are as objectionable as they might appear at first glance. For example, a group called "Skins on Skates" turned out to be nothing more than a klatch of skateboarders with shaved heads.

Other ISPs, such as EarthLink, have a hands-off policy toward objectionable content. "We're pretty much Switzerland," says EarthLink spokeswoman Kirsten Hamling. "We don't monitor what people do, we don't watch where they go." She notes that EarthLink does police itself for obviously illegal content. Yet even if ISPs such as Yahoo and EarthLink completely purge xenophobic content, Stormfront is always waiting in the wings.

The difference between protected and unprotected speech in the United States boils down to whether the speech is a direct, credible threat against a specific target, or a direct incitement to imminent illegal action. There have been prosecutions of online hate speech that appear to cross the line. However, they're usually conducted under the rubric of federal civil rights or fair housing laws.

Last year, a jury awarded $107 million to plaintiffs in a case involving the Nuremberg Files, a Web page that listed names and addresses of abortionists and accused them of crimes against humanity. Three of the doctors were murdered, and their names were crossed out on the page. MindSpring shut down the site, only to be sued for breach of contract by the site's operator, who meanwhile released a CD-ROM version of it.

(Cont'd on next page)

In two federal cases, university students have been convicted of civil-rights violations for sending threatening e-mails to minority groups at their schools (thus interfering with the students' attendance at a public college). In 1998, Richard Machado was convicted of sending threatening e-mail to 60 Asian students at the University of California at Irvine. Last year, Kingman Quon, a California State University at Los Angeles student, pleaded guilty to civil-rights charges and was sentenced to two years in jail for e-mailing threatening messages to Hispanic students, professors and others across the country. And earlier this year, the U.S. Department of Housing and Urban Development settled a housing discrimination complaint against a white supremacist for allegedly using the Web to harass a fair-housing advocate who also served on a hate crimes task force. HUD is funding a national task force that will study online hate speech in a series of meetings nationwide.

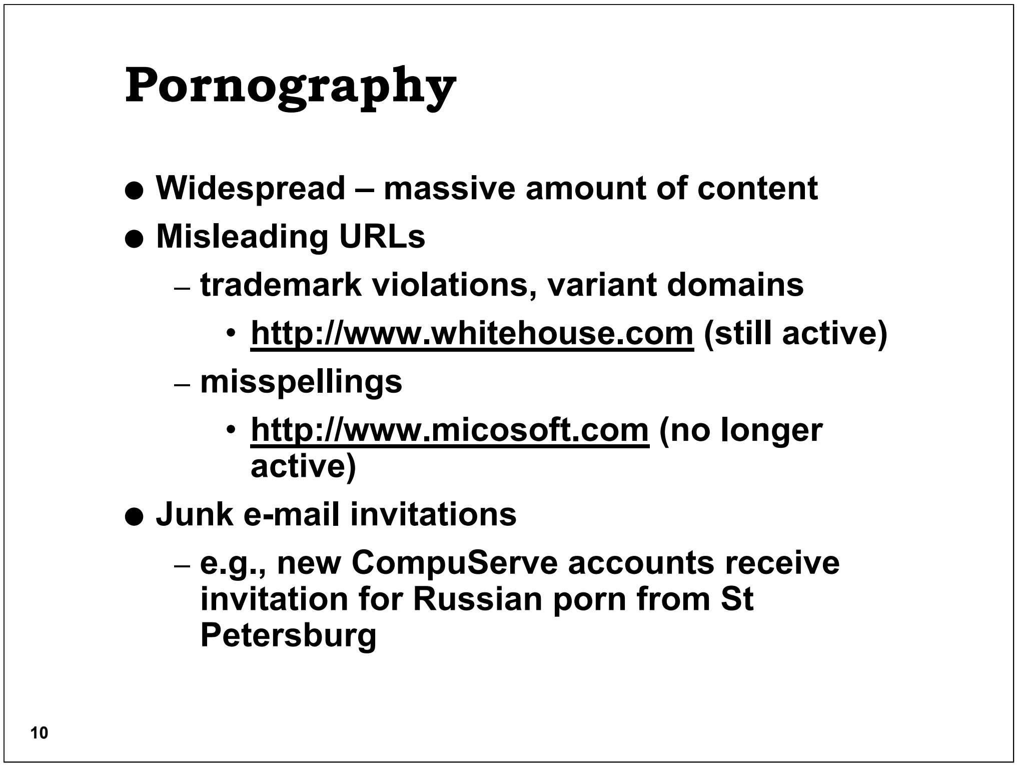
The SPLC's Potok and other antihate advocates contend the Net makes it easier for racists to find each other. The Web removes the need for face-to-face proselytizing and recruiting; xenophobes can now meet and spread their messages globally from the comfort of their homes. They can also reach unlikely new audiences. Black's 11-year-old son, Derek, runs Stormfront for Kids, which includes topics such as Pokemon and videogames, alongside a "history of the white race" and Confederate flag graphics.

Marcus of HateWatch adds that some online hate groups resort to Internet hacking, ranging from e-mail spoofs and denial-of-service attacks to domain name "Webjacking." Some sites even offer downloadable hacking software.

Yale Edeiken, a Pennsylvania historian who rebuts Holocaust deniers, says he has been harassed since 1988. In the wee hours of July 9, several state troopers visited Edeiken's home. They were investigating an online post, apparently by Edeiken, that vowed to destroy an Allentown, Pa., abortion clinic. He didn't send the message, but he has a pretty good idea who hijacked his e-mail address. He'd already launched a civil suit to stop the harassment. The police were "absolutely worthless," grumbles Edeiken, who says the cops wouldn't act on threats alone.

Hatred online won't be eradicated with harsh laws, aggressive software filters or even cybersquatting, which is practiced by some antihate groups. A better method is unflinching exposure and examination. Robert Hilliard, a communications professor at Emerson College in Boston, is planning a fall seminar called "Hate.com." Hilliard says the class is already so popular that it's overbooked.

COPYRIGHT © 2000 Network World, Inc.



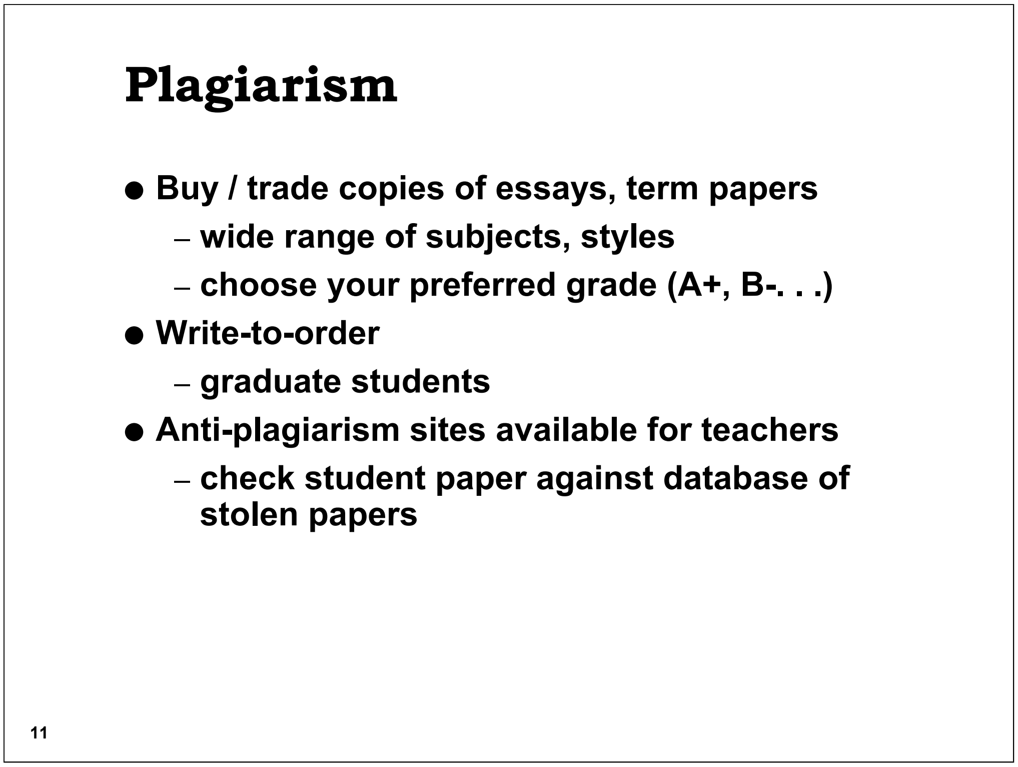
Pornography

- Widespread – massive amount of content
- Misleading URLs
  - trademark violations, variant domains
    - http://www.whitehouse.com (still active)
  - misspellings
    - http://www.micosoft.com (no longer active)
- Junk e-mail invitations
  - e.g., new CompuServe accounts receive invitation for Russian porn from St Petersburg

10

1. Doyle, T. C. (2000). The Architects of Porn: Meet the men and women who push e-business to its extreme. *VARBusiness* (May 1, 2000). http://www.varbusiness.com/Components/Search/Article.asp?ArticleID=16182
2. From *IYIR 2000:*

   2000-03-16 (Newsbytes). In the endless debate between supporters and opponents of Internet filtering (censorware) to prevent kids from seeing pornography, the extreme right-wing Family Research Council (FRC: http://www.frc.org)endorsed a study by David Burt (*Dangerous Access, 2000 Edition: Uncovering Internet Pornography in America's Libraries*) claiming to show that children do in fact access pornography on public library computers. The official position of the American Library Assocation (ALA: http://www.ala.org) is that very few children access pornography on library computers (the ALA's director has said that "only one child out of a trillion billion might use library computers to seek out pornography" -- this despite objections from some working librarians who have come to dread helping users of their terminals for fear of confrontation with various forms of nastiness online). On the other hand, to put things in perspective, the FRC supports homophobia, opposes abortion, objects to First Amendment protection of art museum exhibits, argues that a woman's place is in the home, and describes feminism as having an "unrealized and ironic relationship to the cheapening of life and the value of womanhood, the growth of an overbearing government, and the decline in family and marital stability."

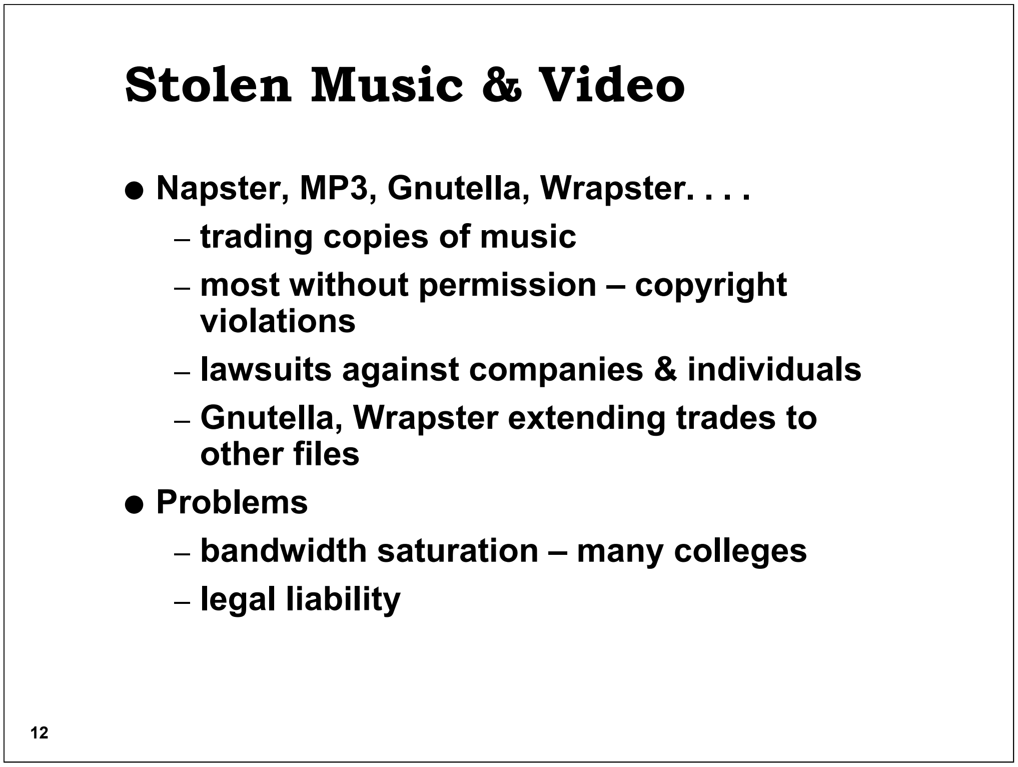


Plagiarism

- **Buy / trade copies of essays, term papers**
  - **wide range of subjects, styles**
  - **choose your preferred grade (A+, B-. . .)**
- **Write-to-order**
  - **graduate students**
- **Anti-plagiarism sites available for teachers**
  - **check student paper against database of stolen papers**

11

EDUPAGE pointed to a report in the New York Times in January 2000 that provided good information on the problem of academic forgery. A variety of anti-plagiarism sites have popped up on the Web to help academics pounce on students who plagiarise material for their essays, term-papers and theses. Some of the useful services are < http://www.plagiarism.org/ >, < http://www.canexus.com/ >, < http://www.cs.berkeley.edu/~aiken/moss.html >, and < http://www.integriguard.com/ >. The engines variously compare student texts (submitted online, of course) with databases of papers, including other student papers and those available on plagiarism sites. Identical or similar passages are highlighted in a written report for the teacher. The technology should not be used as the sole basis for an accusation of plagiarism. [As a university university professor back in 1978, I spotted obvious plagiarism when a dull-witted male student submitted his essay with a cover page that used a different font from that of the rest of the paper. Confronted with my skepticism, he blustered that he had written every word -- even though he could not remember the exact title or any of the content of the paper. But the clincher was language: the French-language paper used the _feminine_ form for all reflexive terms. At that point he broke down.]



Stolen Music & Video

- Napster, MP3, Gnutella, Wrapster. . . .
  - trading copies of music
  - most without permission – copyright violations
  - lawsuits against companies & individuals
  - Gnutella, Wrapster extending trades to other files
- Problems
  - bandwidth saturation – many colleges
  - legal liability

12

(From *IYIR 2000:* NewsScan abstracts used with permission of the authors)

- U.S. District Judge Jed Rakoff . . . [said] MP3.com is using "indefensible" and "frivolous" arguments in its defense against charges of copyright violations brought by the Recording Industry Association of America. The judge, in ruling against MP3.com, determined that the company "is replaying for the subscribers converted versions of the recordings it copied, without authorization, from plaintiffs' copyrighted CDs. On its face, this makes out a presumptive case of infringement." Rakoff called MP3.com's fair-use defense "indefensible" and its claim that it was protecting record companies from music pirates "frivolous." (Bloomberg/Los Angeles Times 5 May 2000)
- [In a related case,] Settling a copyright infringement lawsuit brought against it by Warner Music and BMG Entertainment, the Internet music distribution company MP3.com . . . signed licensing agreements with both those companies. Customers are able to access music in the MP3 database at any time and from any device with Internet access. Warner executive Paul Vidich . . . [said] that the settlement agreement "clearly affirms the right of copyright owners to be compensated for the use of their works on the Internet." (AP/San Jose Mercury News 9 Jun 2000)
- [In September,] . . . federal judge [Jed Rakoff] . . . ruled that MP3.com willfully violated music copyrights and . . . ordered it to pay at least $117 million in damages to Seagram's Universal Music Group -- believed to be the largest copyright infringement penalty in history. "This should send a message that there are consequences when a business recklessly disregards the copyright law," says a senior VP of the Recording Industry Association of America, which represents Universal and the four other major music companies. "We trust this will encourage those who want to build a business using other people's copyrighted works to seek permission to do so in advance." The industry's lawsuit claimed that MP3.com had violated copyright laws by creating a database of 80,000 unauthorized CDs, and the judge's ruling assessed a $25,000 penalty for every Universal CD illegally posted on its My.MP3.com service -- somewhere between 4,700 and 10,000 recordings. MP3.com . . . [said] it will appeal the ruling, which it called "draconian." (Los Angeles Times 7 Sep 2000)

4. Downloading music off the Internet is not stealing in the eyes of 53% of all U.S. Internet users, according to a new study by the Pew Internet & American Life Project. And those who are active downloaders are even more adamant about their position -- 78% do not believe that downloading and sharing files for free is wrong, and 61% don't care if the music they're downloading is copyrighted. Even among the general population, 40% of those surveyed said they didn't see anything wrong with downloading music off the Internet, while 35% said the downloaders are stealing, and 25% chose not to take a position. In a finding guaranteed to raise the ire of the Recording Industry Association of America, only 21% of music downloaders end up actually buying the music they get off the Internet. (E-Commercetimes 2 Oct 2000)

5. Democrat congressman Rick Boucher and three Republican colleagues . . . introduced legislation designed to change the focus of the debate over digital copyright issues from the courts to the legislature. Called the Music Owners' Listening Rights Act of 2000, the bill would legalize the controversial MP3.com music downloading service, which is now defending itself in multimillion dollar lawsuits. Boucher says, "What matters is whether new technologies are consistent with the theory of copyright laws, not just consistent with the details of the copyright law. The law should not stand in the way of an entirely legitimate technology that provides consumer convenience without costing the record companies anything." But Recording Industry Association of America president Hilary B. Rosen thinks that Congress should stay out of the fray and that "I have a hard time believing this is going to get resolved anywhere but in the marketplace." (New York Times 2 Oct 2000)

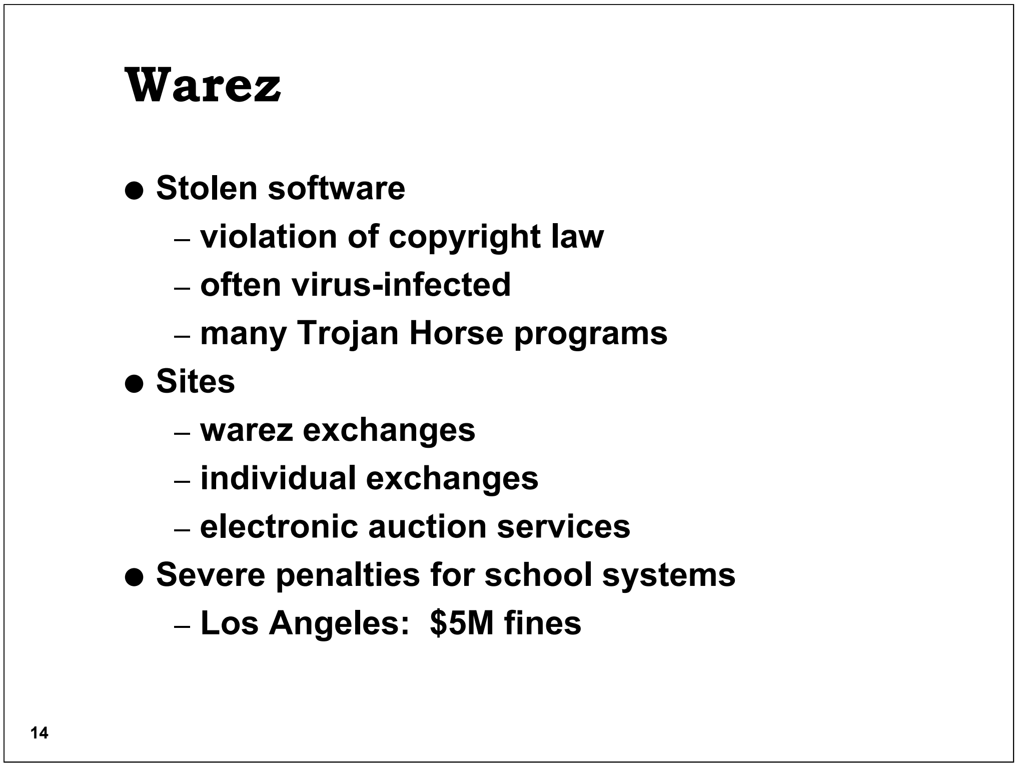
6. **Kabay, M. E. (2000). The Napster Cantata.** http://www.securityportal.com/articles/napster20001013.html

   As we watch the current battles between advocates of free distribution of software and music, it seems to me that we ought to be clear on the arguments being presented by those in favor of such liberation of intellectual property. Perhaps the following ripostes will provide responses to the cant being peddled by these people (or possibly just to generate hate-mail):

- Everyone’s doing it.
- We won’t get caught.
- It’s the music / software industry’s fault: if they don’t want theft, they should charge less.
- It’s the producers’ fault: if they don’t want theft, they should make it technically impossible.
- It doesn’t hurt anyone.
- It only hurts a company — I wouldn’t steal it from an individual.
- The music industry is violating the rights of the musicians, so breaching copyright is a Good Thing.
- Our theft is helping the software / music industry increase their sales.
- No software / music / art should ever be copyrighted — it should always be free.
- But I need it and I don’t want to pay for it.

. . . .

[See the complete article for responses to each excuse.]



Warez

- Stolen software
  - violation of copyright law
  - often virus-infected
  - many Trojan Horse programs
- Sites
  - warez exchanges
  - individual exchanges
  - electronic auction services
- Severe penalties for school systems
  - Los Angeles: $5M fines

14

Newsbytes **May 5, 2000** pNA: **Intel, MS Staff Cited In Pirates With Attitudes Case** 05/04/00. By Martin Stone

CHICAGO, ILLINOIS, U.S.A., 2000 MAY 5 (NB) -- Five employees of giant chip maker Intel Corp. [NASDAQ:INTC] and a former staffer at Microsoft Corp. [NASDAQ:MSFT] are reportedly among those indicted in an allegedly global ring of software thieves.

A Reuters report today said a federal grand jury in Chicago indicted 17 people on Thursday, including two Europeans, for allegedly infringing the copyright on more than 5,000 computer software programs. Of those charged, 12 were suspected members of a group known as "Pirates with Attitudes" (PWA), a software piracy ring infiltrated by government investigators last year.

The PWA site, identified as "Sentinel" or "WAREZ", was located on a computer at the University of Sherbrooke in Quebec and accumulated software that had been stripped of embedded copy protection. The report said that downloadable programs were available to those possessing a secure Internet protocol address and included operating systems, applications like word processing and data analysis, games and MP3 music files.

Reuters said four employees of Santa Clara, Calif.-based Intel shipped hardware to the site in 1998 to boost storage capacity and that they and other Intel employees gained access to the pirated software, which a fifth employee allegedly arranged. An employee of Redmond, Wash.-based Microsoft is alleged to have supplied bootleg copies of Microsoft products for the site, and allegedly gave access to the company's internal net to PWA ringleader, identified as 32-year-old Robin Rothberg, known online as "Marlenus," of N. Chelmsford, Mass., who was charged in Feb. with violating copyrights on thousands of programs. The prosecutors also named alleged PWA members from Belgium and Sweden.

* * *

More on next page

1998-08-13 (EDUPAGE)

It is a commonplace that schools are among the worst violators of copyright law in the US and Canada. Educators often blithely assume that they have implicit dispensation from restrictions on copying. One of the most significant cases of the year occurred when the Business Software Alliance audited the Los Angeles Unified School District and found 1400 illegal copies of proprietary software in a single school in the District. Total costs of replacing illegal software throughout the District may reach $5M.

* * *

Newsbytes April 6, 2000 pNA

Software Piracy Epidemic Could Slow E-Commerce Boom - BSA 04/06/00.

By Adam Creed

SYDNEY, AUSTRALIA, 2000 APR 6 (NB) Hundreds of thousands of "warez and "appz" Web pages providing access to pirated software on the Internet are turning software piracy into an epidemic that could destroy the current e-commerce boom, according to the Business Software Alliance (BSA), an anti-piracy industry group based in Washington DC.

Warez sites make available pirated software for anyone to download, while appz is a term the BSA says refers to pirated applications programs. Another term - "crackz" - refers to details of illegal serial numbers, codes and software patches that bypass copyright protection in software.

The BSA estimates there are 500,000 warez pages, 144,000 appz pages and 46,000 Web pages on the Internet containing crackz.

Speaking in Sydney, Australia today, Robert Holleyman, president and CEO of the BSA, said that the existence of these pages was contributing to a software piracy epidemic worth $1 billion per year in estimated lost revenue and threatening the destruction of the current e-commerce boom.

The solution, Holleyman says is intellectual property protection and enforcement.

While protection is something that the software industry is working on developing itself, Holleyman's idea of enforcement is aggressive and includes:

- stronger laws and penalties, including laws against temporary cocopies stored on the Web, for example, and criminal offences for Internet piracy.

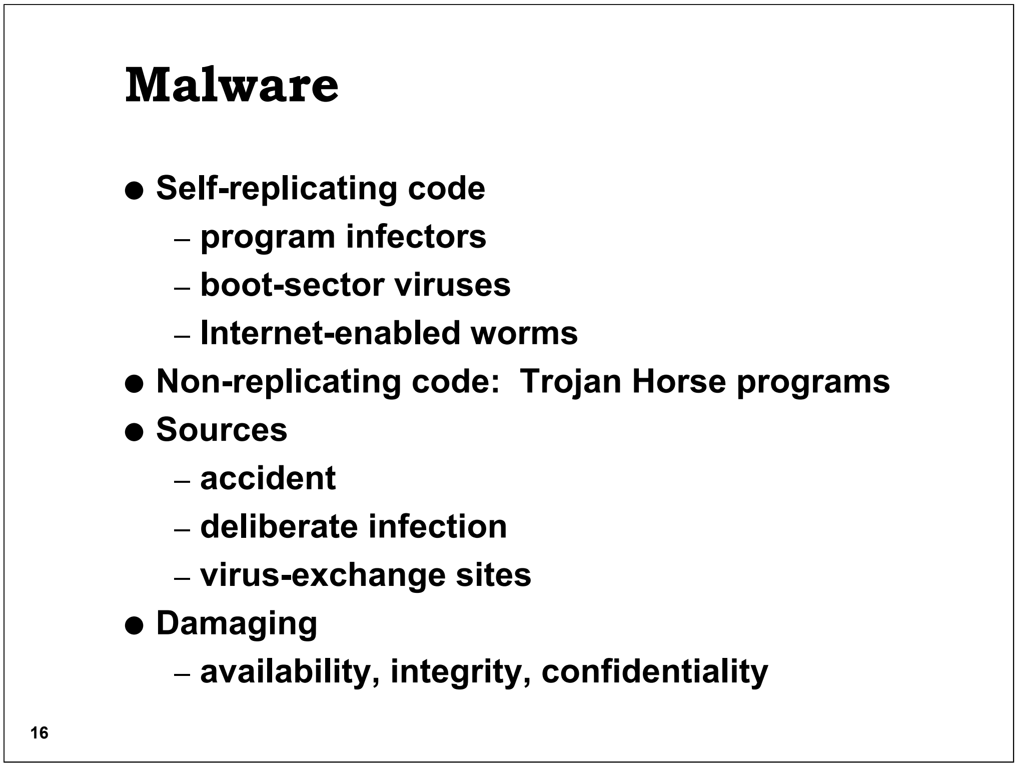
- Persuading domain name registries and Internet service prproviders to reveal the details of those hosting warez sites.

- Liability placed on Internet service providers.

- Laws against reverse-engineering software so that it can be used toto circumvent copyright.

Holleyman said the first step was for governments around the world to ratify the World Intellectual Property Organisation (WIPO) Copyright Treaties.

COPYRIGHT 2000 Newsbytes News Network



Malware

- Self-replicating code
  - program infectors
  - boot-sector viruses
  - Internet-enabled worms
- Non-replicating code: Trojan Horse programs
- Sources
  - accident
  - deliberate infection
  - virus-exchange sites
- Damaging
  - availability, integrity, confidentiality

16

Boardwatch Magazine July 2000 v14 i7 p50

MICHELANGELO MELISSA AND LOVE BUG: The Future of Computer Viruses, Trojan Horses and Worms

By Wallace Wang

On May 4, 2000, the VBS/Love-Letter worm, otherwise known as the Love Bug, became the fastest-spreading computer worm in history, costing an estimated $2 billion to $15 billion to clean up and repair the damage. Not only did the Love Bug worm attack individuals, but it shut down corporate and government e-mail servers, including those belonging to Microsoft, the Pentagon, Ford Motors, the CIA, Lucent Technologies and the British Parliament.

While such widespread devastation captured the headline news, the more important question is, "What can we expect from the virus, worm and Trojan Horse writers of tomorrow?"

DEFINING MALWARE

To understand the Love Bug worm, you need to know the distinctions between the different malware (short for Malicious Software) programs: viruses, worms and Trojan Horses. The main distinction among all three programs is the way they spread.

A virus can only spread by infecting another object such as a program file, a document (like a Microsoft Word file) or the boot sector of a floppy disk. If a virus fails to infect a file, document or floppy disk, it cannot spread.

Unlike a virus, a worm is self-propagating. Worms copy themselves from one computer to another, often without the user's knowledge. Like a virus, a single worm can duplicate itself many times over.

A Trojan Horse program masquerades as another program to trick a person into running it. Once activated, the Trojan Horse distracts the user by displaying a game or message on the screen while it secretly takes some other action such as destroying files or installing programs without the user's knowledge. Unlike a virus or worm, a Trojan Horse cannot make copies of itself automatically.

Cont'd on next page

Note that viruses, worms and Trojan Horses are not inherently destructive, but their surreptitious nature makes them tempting vehicles for spreading trouble. In fact, malware programs often cause damage just through their existence alone. For example, the 1988 Internet worm did nothing but multiply itself from one computer to another, but in the process the worm gobbled up memory and computing resources until grinding a host computer to a halt.

HISTORICAL PERSPECTIVE

Nothing is possible until someone thinks of the idea first. In 1986, that first idea occurred when two brothers from Pakistan discovered that the boot sector of a floppy disk could contain instructions other than loading an operating system. Their program, later dubbed the Brain virus, provided instructions for infecting a computer and spreading to another floppy disk.

Once other people understood how the Brain virus worked, the idea for a virus, that could infect other computers spread faster than the actual Brain virus itself. In this early stage, virus writing required technical knowledge on how computers stored data in memory and retrieved information off floppy disks.

Not surprisingly, macro viruses quickly became the fastest growing virus threat as new variants appeared with frightful regularity. Then in 1999, the Melissa virus appeared.

Unlike other viruses, the Melissa virus didn't passively wait for someone to send an infected file to another computer. Instead, it borrowed characteristics from a worm and actively spread by mailing copies of itself to the first 50 e-mail addresses found in the Microsoft Outlook or Outlook Express address book. The Melissa virus quickly spread throughout the world and became one of the first viruses to appear in international headlines since the Michelangelo virus seven years before.

Then the Love Bug worm appeared, written in another BASIC language variant called Visual Basic Script (VBScript), which is easy to learn, understand and modify. Anyone who receives the Love Bug worm also receives the complete VBScript source code so he can create a new variant of the Love Bug worm right away.

Like the Melissa virus, the Love Bug worm spread itself by using Microsoft Outlook or Outlook Express address books. But where the Melissa virus needed to infect a Word document before it could spread, the Love Bug worm acted independent of any files, mailing itself to every e-mail address stored in an Outlook address book.

The Love Bug worm also combined the social engineering trickery of a Trojan Horse by printing an enticing e-mail subject line. The first version of the Love Bug worm printed ILOVEYOU while later versions displayed the words "fwd: Joke," "Mothers Day Order Confirmation," or a virus alert purportedly issued by Symantec, the publisher of the Norton AntiVirus. In all cases, the e-mail's subject line encouraged its victims to open it, thereby allowing the Love Bug worm to infect the computer.

(To learn how quickly viruses and worms can spread, download the Virus Simulation program from Symantec, www.Symantec.com.)

WHAT THE FUTURE MAY BRING

As viruses and worms become easier to write and even easier to modify, expect to see more copycat macro viruses and worms in the future. Within days of the original Love Bug worm's release, programmers quickly created 29 new variations. Although most changes were as trivial as changing the subject line message, it proved drastic enough to slip past many of the e-mail filters ISPs hastily erected.

As the Love Bug worm spread, the major anti-virus companies released updates to their programs, but updates will always be a knee-jerk reaction to any virus, worm or Trojan Horse threat. Every new virus or worm will always be able to slip past anti-virus programs and wreak havoc until the anti-virus companies have a chance to study the new threat and issue updates to their programs. If you rely on anti-virus programs to protect you, pray that you get the latest update before a new virus or worm finds you first.

No matter what e-mail filters or anti-virus defenses your computer may use, they can never provide 100 percent protection against the most dangerous threats of all, the newest viruses and worms. Both anti-virus programs and e-mail filters can only identify known threats but have no way of detecting any future threats that virus or worm writers might dream up tomorrow. Essentially, this means that every computer on the Internet will always be vulnerable to an attack at any time.

Complicating the situation even more is that viruses, worms and Trojan Horse threats are both a social problem, as well as a technical one. The Love Bug worm could never have spread so quickly if people hadn't been gullible enough to open the file attachment in the first place.

Cont'd on next page

Even worse is that, unlike the Melissa virus, which required the unwitting participation of a victim to share an infected file with someone else, the Love Bug worm could spread itself without having to infect a file first. However, the Love Bug worm did require that victims open the file attachment, but tomorrow's worms may eliminate even this limitation altogether.

According to Michal Zalewski, a Warsaw-based security specialist working for the Internet division of Telekomunikacja Polska SA, a group of programmers worked on such a project to test the feasibility of a worm that could spread without any interaction from the user. The project, called Samhain, halted work last year, but only after creating a successful working prototype. Now that the idea has been proven, expect the next threat to appear as a fully autonomous worm, capable of spreading independent of a user's actions.

Perhaps the best defense against any future, unpredictable attacks is diversity. The Love Bug worm only struck Windows users; Macintosh and Linux users were completely unaffected. Similarly, the Love Bug worm and Melissa virus targeted Microsoft Outlook and Outlook Express users, which meant that Netscape and Eudora users were safely insulated from these two threats, as well.

For the first line of defense, avoid a single standard (such as Windows or even the Linux operating system). This can limit the scope of future malware attacks, but can't reduce the risk of attack completely.

In the old days, people often left their front doors unlocked. Today, hardly anyone ventures out without first locking the front door and sometimes even turning on a burglar alarm, as well.

The computer community has reached a similar crossroads. No longer can we assume that our computers are safe. Instead, we must assume that they will be attacked and prepare ourselves accordingly. This still won't stop a determined intruder, but it can limit trivial attacks, and that by itself can help make the Internet safer for everybody.

MALWARE "MILESTONES"

1986 -- Brain virus: First computer virus released in Pakistan.

1986 -- PC-Write Trojan: First Trojan Horse disguised as a major shareware program, the PC-Write word processor.

1988 -- MacMag virus: First Macintosh virus released.

1988 -- Scores virus: First major Macintosh virus outbreak.

1988 -- Internet worm: First worm to cause widespread haveoc on the Internet, shutting down computers all over the country and making worldwide headlines.

1989 -- AIDS Trojan: First Trojan Horse that held the user's data hostage by encryption the hard disk and demanding that the user pay for the encryption key that would prevent the Trojan Horse from deleting the data.

1990 -- First Virus Exchange Bulletin Board System (VX BBS) appears in Bulgaria where callers could trade live viruses and virus source code through the convenience of a BBS.

1990 -- The Little Black Book of Computer Viruses published by Mark Ludwig. One of the first books to provide detailed instructions and accompanying source code to tech people how to write computer viruses.

1991 -- Tequila virus: First polymorphic virus capable of changing its appearance to avoid detection by anti-virus programs.

1992 -- Michelangelo virus: First computer virus that caused a major media alert. Despite claims that millions of computers were in danger, the Michelangelo virus actually caused relatively little damage.

1992 -- Dark Avenger Mutation Engine (DAME): First toolkit designed to turn any computer virus into a polymorphic virus. Despite its threatening appearance, bugs and its complexity prevent wide-scale use.

1992 -- Virus Creation Laboratory (VCL): First toolkit for creating a virus using pull-down menus.

1996 -- Boza: First Windows 95 virus released.

1996 -- Concept virus: First macro virus released that infects Word documents.

1996 -- Laroux virus: First macro virus released that infects Excel spreadsheet files.

1996 -- Staog virus: First Linux virus released.

1998 -- Strange Brew virus: First Java virus released.

1998 -- Back Orifice: First remote administration Trojan Horse that allows others to completely take over a target computer through the Internet.

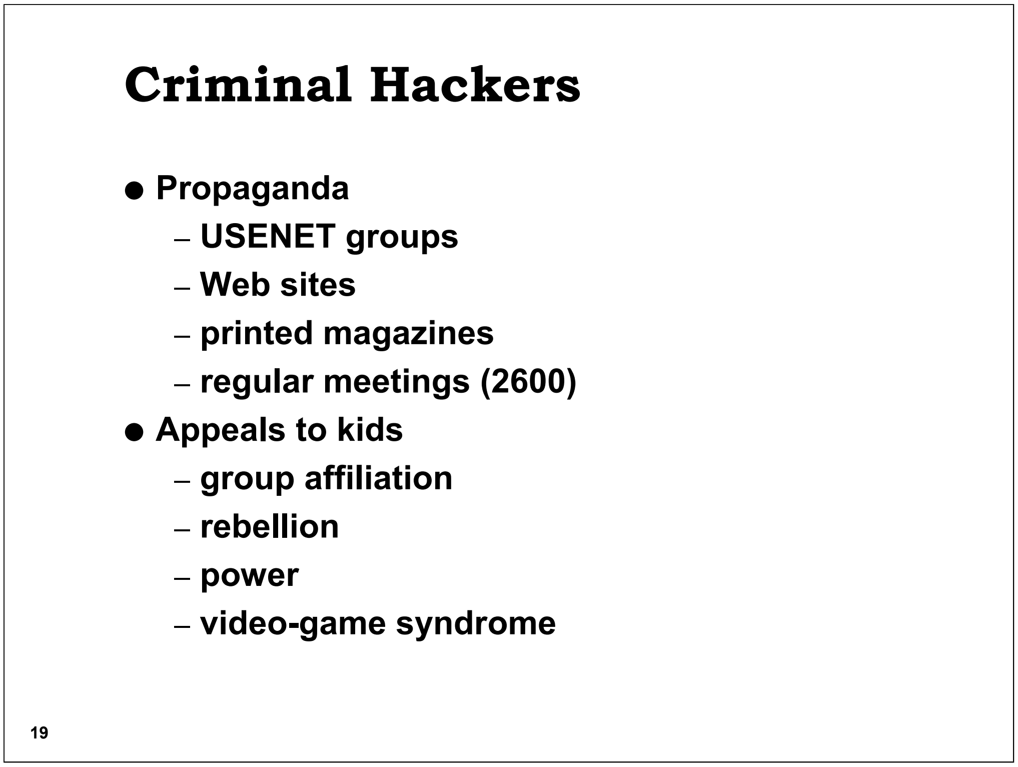
1999 -- Melissa virus: First virus to spread by e-mail through Microsoft Outlook and Outlook Express address books.

1999 -- Tristate virus: First macro virus capable of infecting Word, Excel and PowerPoint files.

2000 -- First large-scale denial of service attacks to shut down major Web sites including Yahoo!, Amzon.com, CNN and eBoy.

2000 -- Love Bug worm: The fastest spreading worm in history, causing an estimated $2 to $15 billion in damages.

COPYRIGHT 2000 Boardwatch Magazine



Criminal Hackers

- Propaganda
  - USENET groups
  - Web sites
  - printed magazines
  - regular meetings (2600)
- Appeals to kids
  - group affiliation
  - rebellion
  - power
  - video-game syndrome

19

1. Every course on information technology should include discussion of ethical issues. For a basic overview of the ethical implications of computer use, see

   Kabay, M. E. (2000). Why Kids Shouldn't Be Criminal Hackers, v07. http://securityportal.com/cover/coverstory20001009.html

2. For an adult perspective on integrating cyberspace into our moral universe, see

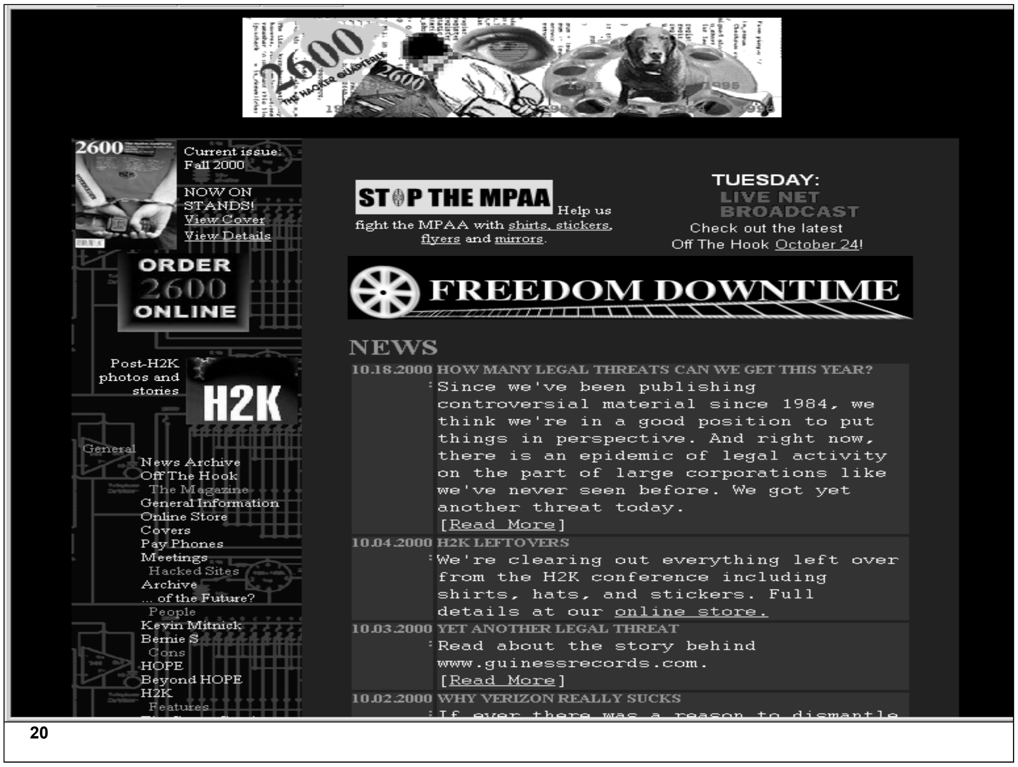
   Kabay, M. E. (1996). Totem and Taboo in Cyberspace.

   http://www.icsa.net/html/library/whitepapers/Totem_Taboo_Cyberspace.pdf

3. The video-game syndrome is the belief that because video games and computer hacking resemble each other in the use of keyboards, monitors, modems and the Internet, therefore breaking into systems is really just a game that harms no one. Children do not know that there are human beings on the other end of their depradations who are forced into sleepless nights and psychological stress when intruders tromp through their production systems.

4. For a discussion of ethical decision-making suitable for high-school students and teachers, see

   Kallman, E. A. & J. P. Grillo (1996). *Ethical Decision Making and Information Technology: An Introduction with Cases, Second Edition.* ISBN 0-07-034090-0. xiv + 138. Index.



2600 Current issue: Fall 2000

NOW ON STANDS!
View Cover
View Details

ORDER 2600 ONLINE

Post-H2K photos and stories

H2K

General
News Archive
Off The Hook
The Magazine
General Information
Online Store
Covers
Pay Phones
Meetings
Hacked Sites
Archive
... of the Future?
People
Kevin Mitnick
Bernie S
Cons
HOPE
Beyond HOPE
H2K
Features

STOP THE MPAA Help us fight the MPAA with shirts, stickers, flyers and mirrors.

TUESDAY:
LIVE NET BROADCAST
Check out the latest
Off The Hook October 24!

FREEDOM DOWNTIME

NEWS

10.18.2000 HOW MANY LEGAL THREATS CAN WE GET THIS YEAR?
: Since we've been publishing controversial material since 1984, we think we're in a good position to put things in perspective. And right now, there is an epidemic of legal activity on the part of large corporations like we've never seen before. We got yet another threat today.
[Read More]

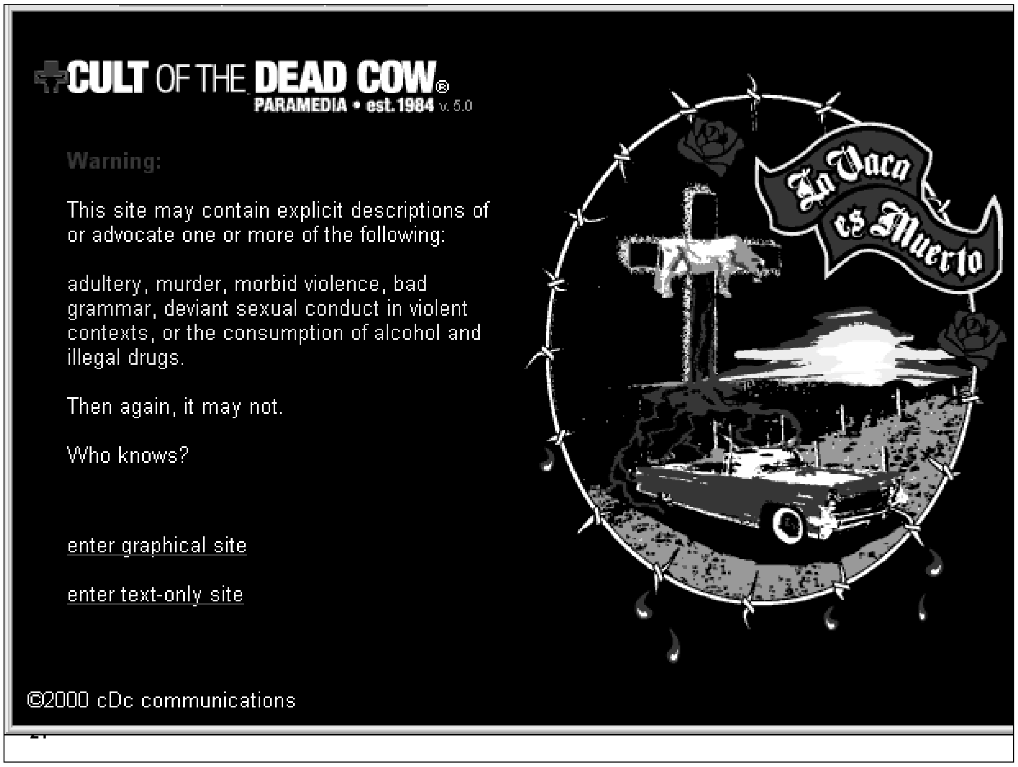
10.04.2000 H2K LEFTOVERS
: We're clearing out everything left over from the H2K conference including shirts, hats, and stickers. Full details at our online store.

10.03.2000 YET ANOTHER LEGAL THREAT
: Read about the story behind www.guinessrecords.com.
[Read More]

10.02.2000 WHY VERIZON REALLY SUCKS
: If ever there was a reason to dismantle

1. Eric Corley is the editor of *2600: The Hacker Quarterly* and detests being called by his real name (so I always do so). His pseudonym is Emmanuel Goldstein.
2. The 2600 magazine and Web site < www.2600.com > are notorious for publishing detailed attack scripts (exploits) that allow even children to use some attack methods on unprotected sites. The tone of the articles is uniformly puerile, with pretensions to anarchism and much exploitation of the hacker propaganda that circles among adolescents in the geek crowd.
3. 2600 has chapters around the world; members meet on the first Monday of every month
4. Corley is currently in legal trouble for having posted information about DeCSS, a program for cracking the restrictive codes that limit playback of DVDs to specific regions of the world.
5. Some other sites by or about criminal hackers (visit these using a personal firewall; don't accept cookies; don't accept JAVA scripts from these sites – and don't give them any information about yourself):
   - www.antionline.com
   - www.attrition.org
   - www.freshmeat.net
   - www.hackershomepage.com
   - www.hackernews.com
   - www.phonelosers.org
   - www.phrack.com
   - www.sd2600.com
   - www.segfault.org
   - www.slashdot.org
   - www.veridian.com

Copyright © 2001 M. E. Kabay. All rights reserved.



CULT OF THE DEAD COW®
PARAMEDIA • est.1984 v.5.0

Warning:

This site may contain explicit descriptions of or advocate one or more of the following:

adultery, murder, morbid violence, bad grammar, deviant sexual conduct in violent contexts, or the consumption of alcohol and illegal drugs.

Then again, it may not.

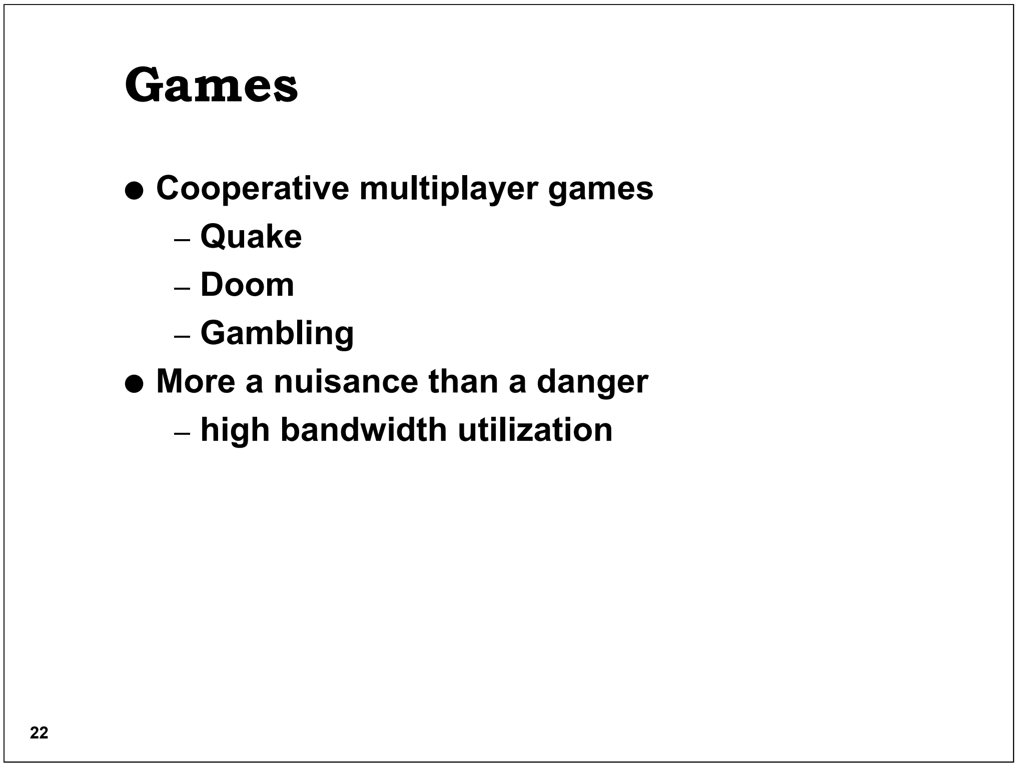
Who knows?

enter graphical site

enter text-only site

©2000 cDc communications

1. The cDc is more like a performance-art collective than a criminal conspiracy. Members sport names such as Deth Vegetable. However, some of their members have released harmful software such as BackOrifice and BackOrifice2K.
2. From the *IYIR 1999*: **1999-07-12 (AP).** The Cult of the Dead Cow released BackOrifice 2K (B02K), the newest version of its 1998 penetration tool, BackOrifice (named as a lampoon of the BackOffice product of Microsoft). BO2K, usually installed illegally on victim machines through a contaminated vector program that has been thereby transformed into a Trojan horse, allows complete remote control and monitoring of the infected PCs. BO2K was noteworthy because it attacks WindowsNT workstations and servers and thus has even more serious implications for INFOSEC. Anti-virus companies worked feverishly immediately after the release of the tool to update their virus-signature files. A criminal hacker calling himself Deth Veggie insisted that the CDC is involved in guerilla quality assurance — their penetration tools, he argued, would force Microsoft to repair the "fundamentally broken" Windows operating systems. Jason Garms, lead product manager for Windows NT security, disagreed strongly: "I certainly categorize what they're trying to do as being malicious. This program they have created has absolutely no purpose except to damage users." He added, "You can't walk down the street and pick up a rock and throw it through someone's window. You'd be arrested. But there are people on the Internet that would.



Games

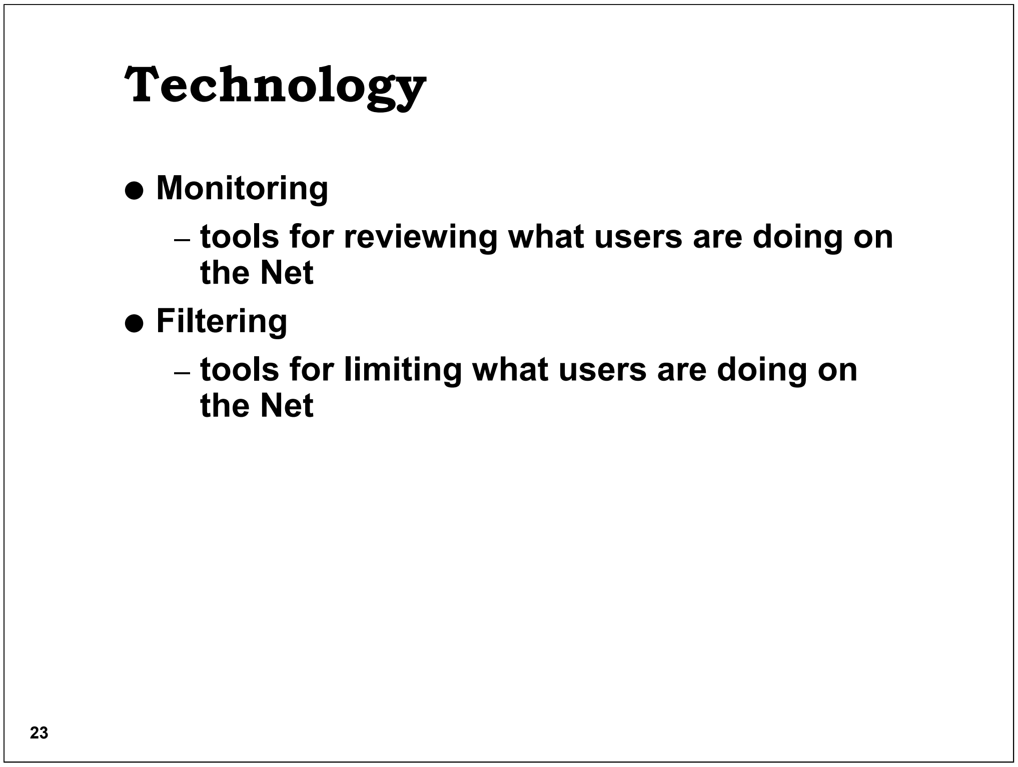
- Cooperative multiplayer games
  - Quake
  - Doom
  - Gambling
- More a nuisance than a danger
  - high bandwidth utilization

22

Los Angeles Times: Feb 10, 2000: **Fantastic, adults-only 'Quake III' shakes up violent shootout genre.**Quake III arena is a violent game for adults who know the difference between fantasy and reality, right and wrong. Players advance by killing a predetermined number of opponents, all of whom have individual personalities and fighting styles. The game can be played in standalone against the computer, or over a network against remote players.

* * *

NewsScan: **INTERNET GAMBLING ON THE RISE.** The number of cybercasinos has ballooned from 15 in 1996 to more than 700 today, with revenue estimated to reach $1.5 billion this year, and $3 billion by 2002, according to an analyst for the online gambling industry. And despite government moves to criminalize online gambling, U.S. citizens account for about 50% of the industry's revenues. Using the Internet for sports-wagering is already banned, and the Senate passed the Internet Gambling Prohibition Act last year, which would make it illegal to bet on casino-style games online. A companion bill is pending in the House and will be the subject of a subcommittee hearing on March 9. (AP/Los Angeles Times 28 Feb 2000). http://www.latimes.com/wires/wbusiness/20000228/tCB00V0457.html



Technology

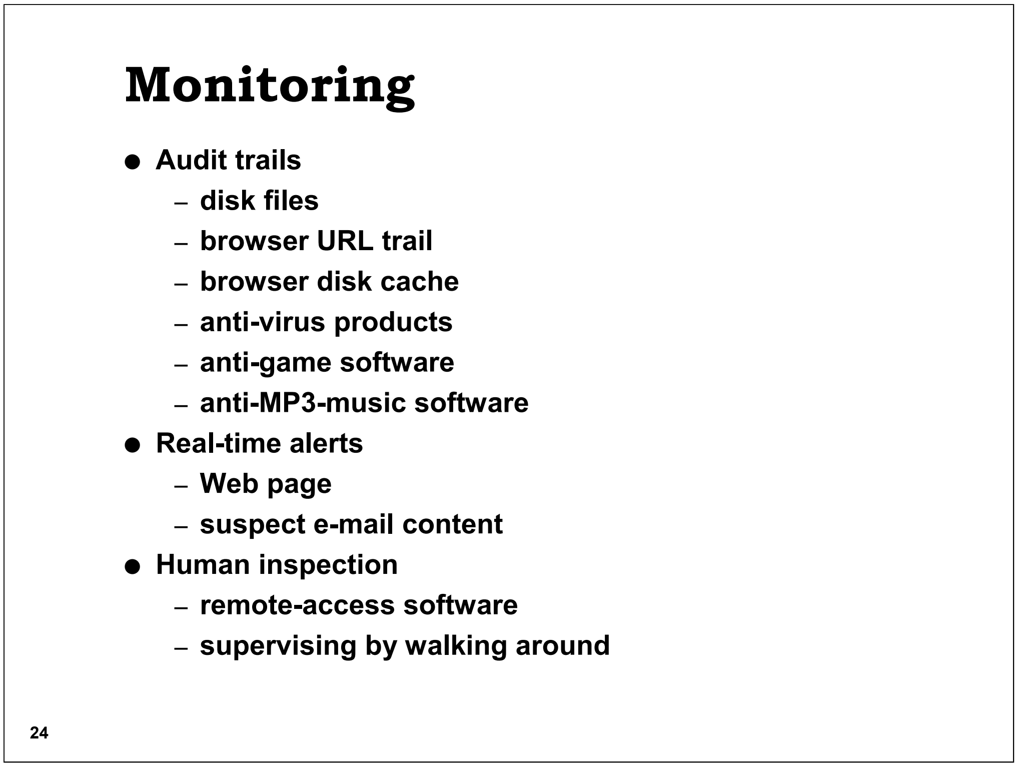
- **Monitoring**
  - **tools for reviewing what users are doing on the Net**
- **Filtering**
  - **tools for limiting what users are doing on the Net**

23

1. Keeping track of what users do on corporate systems is useful only if
   a. There are clear policies in place defining acceptable use; and
   b. Users have no expectation of privacy in using the corporate systems.
2. Filtering content is far more problematic than monitoring or auditing access.
   a. Technology is currently crude
   b. False positives (rejection of harmless sites) is common
   c. Public funding of institutions decreases tolerance for censorship

3. See Peeping tools: Berkley, T. (2000). Nine tools that can snoop on your employees. *Network World*, (2000-07-10)

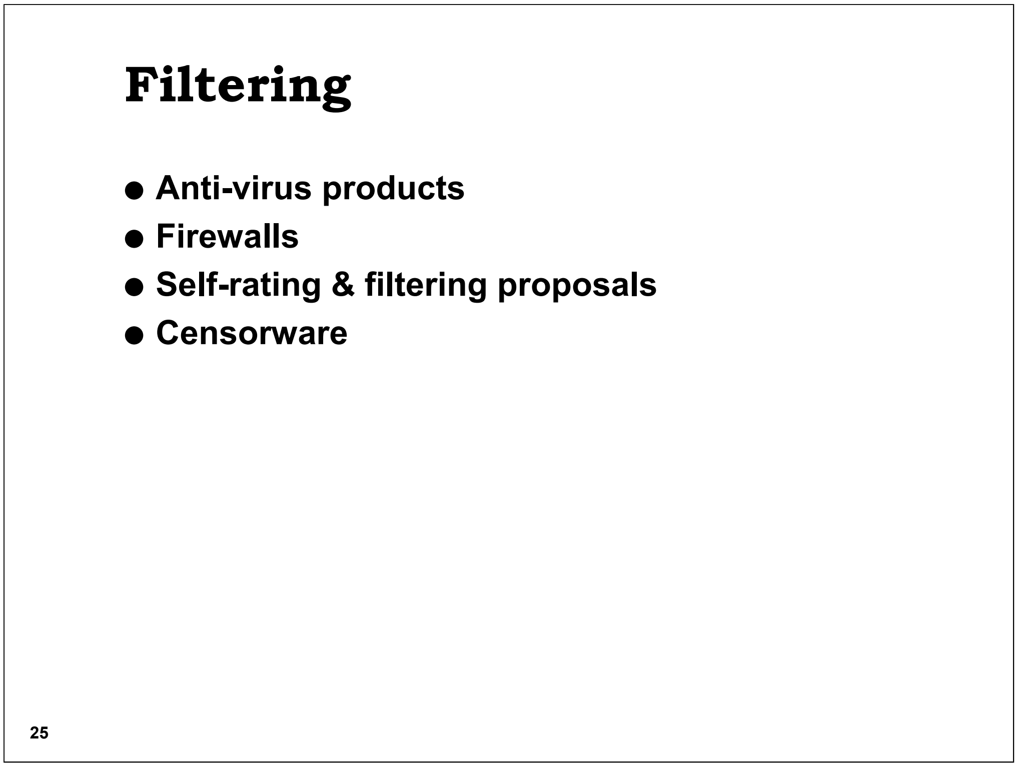
http://www.nwfusion.com/research/2000/0710feat.html for an extensive analysis of software that keeps and analyzes audit trails of employee (or family) Web usage.



Monitoring

- **Audit trails**
  - **disk files**
  - **browser URL trail**
  - **browser disk cache**
  - **anti-virus products**
  - **anti-game software**
  - **anti-MP3-music software**
- **Real-time alerts**
  - **Web page**
  - **suspect e-mail content**
- **Human inspection**
  - **remote-access software**
  - **supervising by walking around**

1. Some products search for unauthorized software such as games or unauthorized materials such as pornography.
2. Each browser usually keeps a cache on disk which can be searched. Browsers also have history lists of all URLs visited. However, these are all easy to clear by the user.
3. Anti-virus products usually have log files that show which viruses were identified and what the product did with them.
4. Specialized anti-game products search out thousands of known games and identify their files even if filenames are altered; e.g., AntiGame Plus by DVD Software < http://www.antigame.com/ >
5. Anti-music-file programs ferret out stored MP3 files; e.g., SoundJudgment < http://www.antigame.com/products/soundjudgment.shtml >
6. Some programs provide e-mail alerts to supervisors when suspect material in accessed or received; e.g., SuperScout by surfControl, < http://www.surfcontrol.com >.
7. Remote-access software allows simultaneous view of a target system by a supervisor; e.g., CarbonCopy < http://www5.compaq.com/services/carboncopy/ > or pcAnywhere < http://enterprisesecurity.symantec.com/products/products.cfm?productID=2 >).

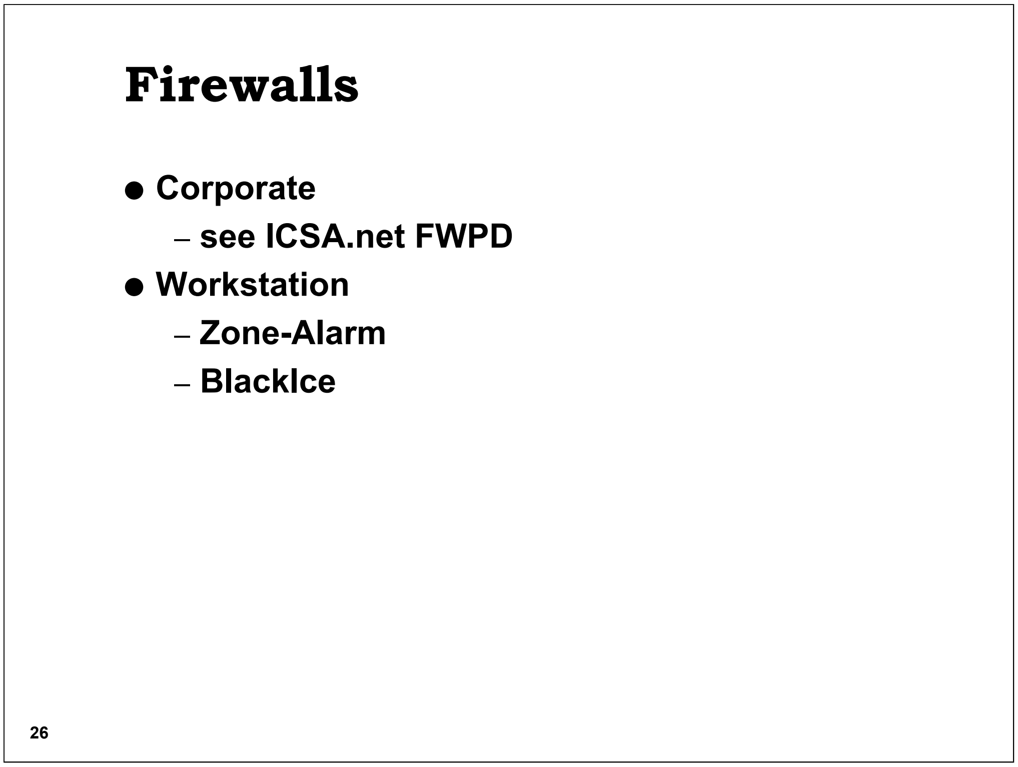


Filtering

- Anti-virus products
- Firewalls
- Self-rating & filtering proposals
- Censorware

25

1. Filtering focuses on stopping transmission or executions of materials that are not authorized by specific policies.
2. Anti-virus systems identify malicious software either using
   - signatures (characteristic sequences of computer code); or
   - generic malicious behavior (e.g., requests for writing to a boot sector).
3. Firewalls implement policies on what kinds of packets are allowed into (and sometimes out of) a network connected to the Internet or to any other (e.g., internal) networks.
4. There are proposals under discussion for automatic recognition of ratings applied to Web sites much as ratings are applied to movies, music and video games.
5. Software that automatically blocks access to specific sites or which block specific content is sometimes(derisively) known as *censorware.*



Firewalls

- Corporate
  - see ICSA.net FWPD
- Workstation
  - Zone-Alarm
  - BlackIce

Network World May 15, 2000 pNA

Blocking Napster and RealAudio/Video

By Ron Nutter

I am tired of people using Napster and ReadAudio/Video on my Internet connection because it is illegal and it ties up a lot of bandwidth. Using a firewall or router configuration, how can I successfully block Napster or RealAudio/Video traffic?

I have a Cisco 261x router and a Novell Border Manager 3.5 Enterprise Edition firewall.
--Via the Internet

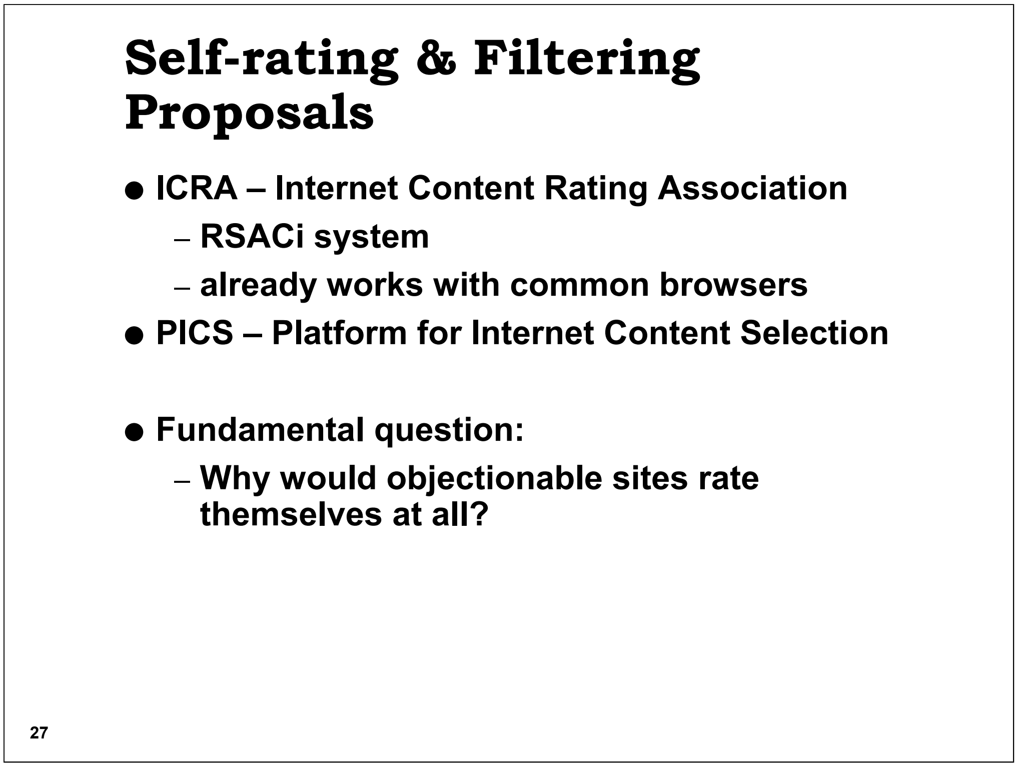
* * *

You have two options. Probably the easiest to control would be to handle things through the Border Manager firewall. You can use filters to control what can get into and out of your network. By using the Filtcfg.nlm, you can limit what traffic is allowed to pass through the firewall from one interface to another. I have worked with packet filtering on several revs of Border Manager and things have become a little easier to work with in later versions.

Setting up filters on Border Manager is part science and part art. Novell Advanced Technical Training has released a video and CD that detail how to implement packet filters. You can also get an electronic book about packet filtering in PDF form from www.caledonia.net. You can use the access rules to control down to a port level who can send what type of traffic. By using the access rules and the single signon within Border Manager, you can get a log that tells you exactly who is trying to send and receive what kind of traffic.

Novell also has ZEN for Networks, which lets you filter at the Cisco router with NWAdmin, which is more user-friendly. ZEN also lets you prioritize traffic types, such as e-mail, so that bandwidth is always available.

COPYRIGHT 2000 Network World, Inc.



Self-rating & Filtering Proposals

- ICRA – Internet Content Rating Association
  - RSACi system
  - already works with common browsers
- PICS – Platform for Internet Content Selection
- Fundamental question:
  - Why would objectionable sites rate themselves at all?

27

Internet Content Rating Association: http://www.icra.org/

The Internet Content Rating Association is an international, independent, non-profit organization with offices in Washington, D.C, USA and Brighton, UK, that empowers the public, especially parents, to make informed decisions about electronic media by means of an open, objective, content advisory system. The RSACi system managed by ICRA provides consumers with information about the level of sex, nudity, violence, offensive language (vulgar or hate-motivated) in Web sites. To date, RSACi has been integrated into Microsoft's browser, Internet Explorer, and MicroSystem's Cyber Patrol Software. CompuServe (US and Europe) has also committed to rate all its content with the RSACi system.

Rating The Web

Our aim in creating RSACi (RSAC on the Internet) was to provide a simple, yet effective rating system for web sites which both protected children and protected the rights of free speech of everyone who publishes on the World Wide Web.

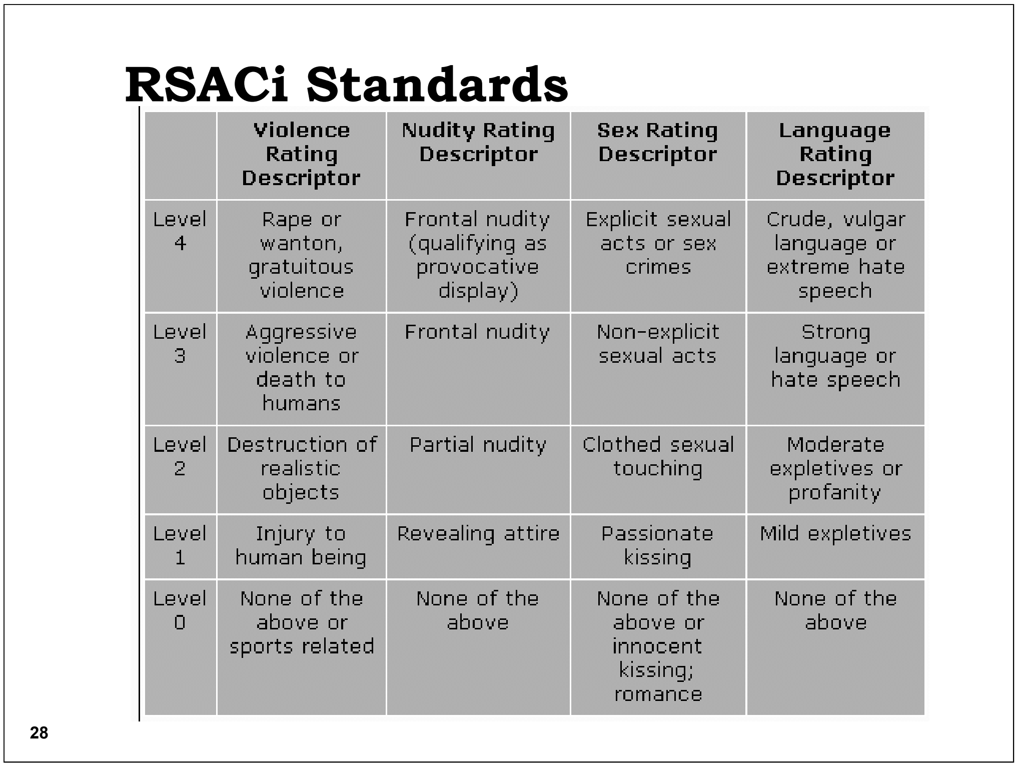
Parental Controls

We also designed a system based on the tried and tested content advisory system used for computer games and one which could be simply understood and set by parents at either the browser level (eg. Microsoft's Internet Explorer 3.0x) or blocking device (eg. CyberPatrol). We urge parents, educators and other interested individuals to SET THE LEVELS at the growing number of browsers and software devices that are designed to read the RSACi labels.

Content Providers

Another essential part of this highly ambitious task, is to encourage internet content providers of all kinds to use our voluntary, self-disclosure rating system. There are a number of compelling reasons why a provider or web master would rate with RSACi, not least that it sends a clear signal to governments around the world, that the World Wide Web is willing to self-regulate, rather than have the heavy hand of government legislation decide what is or is not acceptable.

(Cont'd on next page)



RSACi Standards

	Violence Rating Descriptor	Nudity Rating Descriptor	Sex Rating Descriptor	Language Rating Descriptor
Level 4	Rape or wanton, gratuitous violence	Frontal nudity (qualifying as provocative display)	Explicit sexual acts or sex crimes	Crude, vulgar language or extreme hate speech
Level 3	Aggressive violence or death to humans	Frontal nudity	Non-explicit sexual acts	Strong language or hate speech
Level 2	Destruction of realistic objects	Partial nudity	Clothed sexual touching	Moderate expletives or profanity
Level 1	Injury to human being	Revealing attire	Passionate kissing	Mild expletives
Level 0	None of the above or sports related	None of the above	None of the above or innocent kissing; romance	None of the above

28

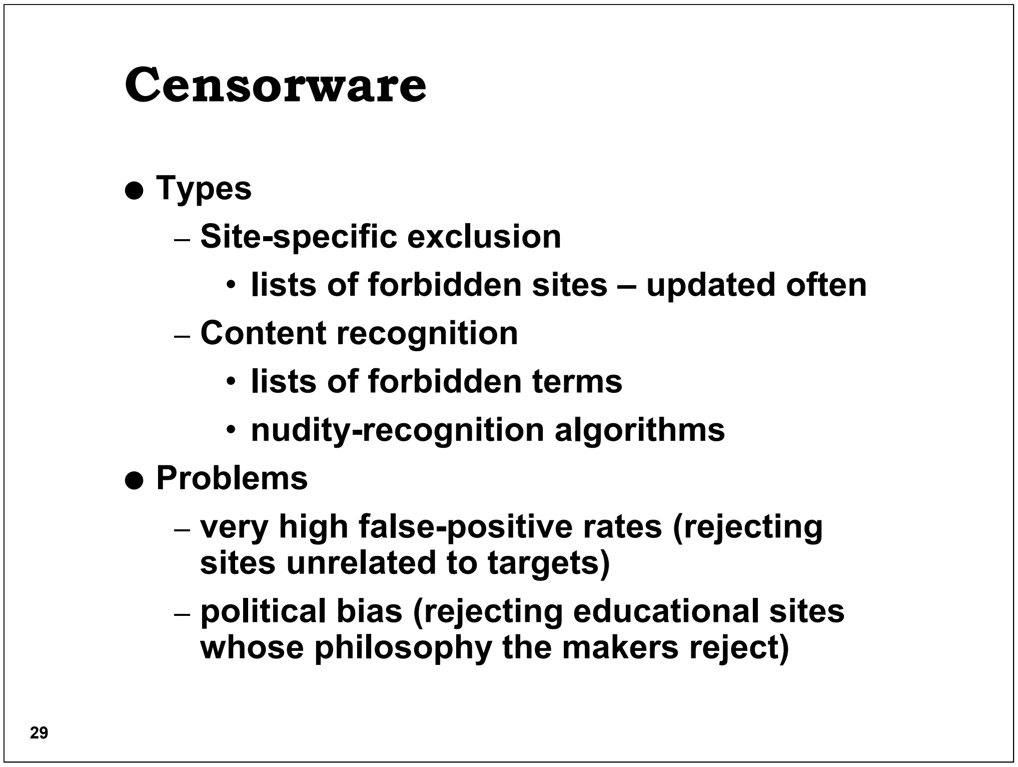
(Cont'd from preceding page)

Commercial Web Sites

Commercial sites, with little or no objectionable material will want to rate. When a parent sets the levels for their child, they will also be offered an option that says, "Do not go to unrated sites". Most sites want the maximum number of visits to justify advertising or other related commercial activity. It would make good marketing sense for all commercial sites to rate whether or not they have any content that could be described as harmful.

Protecting Free Speech

RSACi has been an enthusiastic member of a number of initiatives that would support the protection of free speech on the Web. We work closely with PICS, the Platform for Internet Content Selection, based at MIT. This standard format provides us the means by which our rating system can be read by browsers and selection software around the world.



Censorware

- Types
  - Site-specific exclusion
    - lists of forbidden sites – updated often
  - Content recognition
    - lists of forbidden terms
    - nudity-recognition algorithms
- Problems
  - very high false-positive rates (rejecting sites unrelated to targets)
  - political bias (rejecting educational sites whose philosophy the makers reject)

1. For a comprehensive list of links to 42 specific filtering products and children's poirtals, see http://www.netparents.org/parentstips/browsers.html
2. Censorship algorithms are constantly in the news as yet another laughable error comes to light; e.g., AOL subscribers attempting to enter their home town of Scunthorpe, England were rejected by a very stupid algorithm. Sites on breast cancer have been barred by various products, as have a wide range of unobjectionable sites using legitimate terms that happen to be in use with banned meanings in other contexts.
3. Certain software manufacturers have barred sites that were critical of their products; others barred sites such as the National Organization of Women, gay and lesbian support sites, and so on.
4. Recent research has resulted in algorithms that can identify nudity using recognition of curves and skin tones; these algorithms should be incorporated into commercial filtering products to identify inappropriate graphics on disk and in e-mail:

   Software Does The Censoring So You Don't Have To ---- Diane Rezendes Khirallah

   InformationWeek 2000-09-22

   http://www.informationweek.com/story/IWK20000922S0007

   You can't judge a book by its cover, but can you judge an attachment by its color? Content Technologies thinks so. It's pushing a new product called Pornsweeper that automatically scans each incoming E-mail image, measuring the percentage and proportion of skin tones to other colors in the image.

   If too much flesh is detected (as set by buyers of Pornsweeper), the program blocks the E-mail, assuming it's carrying sexually explicit material. If administrators prefer, tagged messages can spur an automatic response to the recipient, the sender, or administrators.

   Pornsweeper could become a very popular tool for IT. According to some analysts, most online porn is downloaded between 9 a.m and 5 p.m.

   But, you might well ask, what about the many E-mailed images of pigs with humanlike skin tones? The company's Web site states that the software "should be able to differentiate between the skin color of pigs as opposed to the skin color of humans, unless, of course, the pig had very humanlike skin color."

WinMag.com July 7, 2000

Keep An Eye On Your Store

By Karen J. Bannan

Whoever said ignorance is bliss didn't have employees or children with Internet connections. Today, not knowing what users are doing can have dire results. There are several programs available to block access to questionable or offensive material, but few actually block access, log activity, and present information in a coherent manner. Pearl Software's Cyber Snoop 4.0 is one such program that does. (click to see larger image) You can decide how little-or much-you want users to see online. Cyber Snoop not only lets you monitor what PC users are looking at and doing, it also lets you limit them to specific sites or to no Web access at all.

Some blocking software requires you to block all the sites on a specific set of lists. Cyber Snoop lets you block just a single site if that's what you want. This feature isn't just for Web browsing. You can also do the same with chat, newsgroup, and e-mail activity.

The program's logging capability captures and logs everything a user a user does online-e-mail, instant message chat clients, Web-based e-mailing, posting to newsgroups, filling out forms. This means that if you have a PC shared by multiple users, you know which employee is hitting the porn sites at lunchtime. It also means that you can see if your employees are chatting with headhunters or if your spouse is up to no good while you sleep at night. Since users tend to be cautious when they know they are being watched,

I liked the fact that the monitoring process is completely undetectable--unless you want it to be noticed. The program allows you to select whether or not users know if they've violated a rule. With custom violation messages such as "These sites are off limits," you can ram home the fact that the violator is busted.

When testing the program, I set all the defaults to the most restrictive settings. First, I tried to thwart the program by going to relatively innocuous sites that have rather damaging URLs. For example, I went to the parody/online game, which uses a URL that's only a few letters off from the FastCompany.com name. Technically, it should've been banned since the URL does contain profanity. However, since I didn't specifically designate the site as off-limits, I cruised right in. Of course, my activity was logged; if an employer, spouse, or parent wanted to, they could set a block for next time. As soon as I turned on the pre-formatted ratings lists, I was immediately banned from the site and received my custom blocking message and a Network Error to let me know I had strayed.

After adding several friends' names to the chat blocking feature, I fired up my AOL Instant Messenger program. I saw one of the names on my Buddy List and tried to message my friend. Blocked again! If I was able to get in, the program will also log a full-text version of all chats, e-mails, and newsgroup postings that aren't blocked.

I also set time constraints, limiting my online usage to an hour. Sure enough, the program diligently let me know when my time was up. Cyber Snoop lets you designate when users can be online in hour chunks; and you can set limits by day of week, a nice tool for anyone who pays for bandwidth and doesn't want employees surfing overtime. (click to see larger image) A list of everyplace a user has been is displayed, complete with URL and descirption.

When finished cruising around the Web, I checked on my activity. Every place I had visited and everything I'd done was right there, complete with URL and description. This newest version also supports encryption, so your children's personal information is kept private. Although I believe strongly in personal privacy and freedom, as I was using the program I could see how and why people would use software like this.

I did wish that it was a little easier to use. The Help files weren't much help, especially when I first got started. The wizard did help me set up the program, but I still had to root around in the online manual before I realized how to add words and Web sites to my blocked list. The less-than-stellar user support is the main reason the software doesn't make the WinList. However, the wonderful logging capabilities and outstanding filtering and monitoring make Cyber Snoop 4.0 a smart download for almost anyone who needs to do a little online detective work.

Copyright © 2000 CMP Media Inc.

Network Computing Feb 21, 2000 p55

Regulating Web Surfing

-- Need to control Web usage? We tested seven content monitors that can keep even the most adept browser from spending his or her days surfing on the job.

By Gregory Yerxa

. . . .SurfControl's SuperScout won our Editor's Choice award with the most comprehensive policy creation and enforcement options. Combined with solid real-time monitoring and a plethora of supported reporting formats, it narrowly edged out Elron Software's CommandView Internet Manager. Although Internet Manager offers extremely informative reports, its flexibility falls short of that offered by SuperScout.

SurfControl's LittleBrother also fared well, with excellent real-time monitoring features and informative reports. The remaining offerings failed to measure up in at least one area and may be more well-suited for installations that can overlook their shortcomings. Internet Products' iPrism and N2H2's Internet Content Management Appliance will fit well in installations that prefer an appliance to a specialized server or workstation. Websense's Websense Enterprise and Secure Computing's SmartFilter round out our group with average policy creation and enforcement, and average monitoring capabilities.

HTTP remained the most common and most easily restricted traffic type, though some of the products can monitor and inspect traffic types beyond HTTP, including SMTP, NNTP (Network News Transfer Protocol), FTP and telnet at a minimum.

We focused on two types of products in our tests: Internet Content Management Appliance, SmartFilter, SuperScout and Websense Enterprise act as proxy servers, requiring all client traffic to be directed through them, while Internet Manager and LittleBrother transparently monitor the network traffic via an Ethernet bridge or software network traffic sniffer or analyzer. iPrism works both ways. Although both types of products proved equally proficient at monitoring and blocking network traffic in our tests, each type has benefits and drawbacks. For example, proxy-based solutions require all client machines to be configured to use the proxy machine and are limited to monitoring network protocols capable of being proxied. This restricts monitored traffic to stateful protocols such as HTTP and FTP, which let the proxy act on behalf of the client for the duration of any transaction between client and server.

Transparent products avoid this limitation but they require a particular network configuration, such as a non-switching network hub or Ethernet bridge, to inspect network traffic. They also may be at risk for performance limitations, as we discuss in "How We Tested," below. iPrism's hardware-based solution fits both spaces because it can act as a transparent Ethernet bridge or an application proxy. With the exception of iPrism and N2H2's Internet Content Management Appliance, the other products are software-based. Most of the software products also are available as plug-ins to popular proxy servers, including those from Microsoft Corp. and Netscape Communications Corp., as well as Check Point Software Technologies' FireWall-1. During our testing, however, we did uncover some shortcomings of nonproxy-based, or transparent, content monitoring solutions such as iPrism (in transparent mode), SurfControl and Internet Manager.

How We Tested

We installed and configured each product to monitor and block Web traffic on our production network. We then configured each product to block traffic to unproductive or "improper" sites while letting productive uses of Web, e-mail and FTP traffic go past. In the case of iPrism, Websense Enterprise and Internet Content Management Appliance, content rules were determined by the provided service databases. We visited a broad range of improper Web sites to evaluate each product's content policies and, if applicable, dynamic policy rules.

All products behaved as expected when they worked with only a few clients. We performed heavy-use tests with 12 additional workstations and a Web server configured with static content on the local LAN. The workstations were configured to grab Web content as fast as possible from the source server. We used an additional client to access sites that during previous tests had resulted in a blocked site.

(Cont'd on next page)

It quickly became evident that these products were not capable of handling traffic at Fast Ethernet speeds in either mode. In all cases the products performed significantly slower; in extreme cases their performance ground to a halt and even sometimes required a few minutes to recover. Proxy-based solutions fared better, though service through the proxies was significantly slower at higher speeds. Nonproxy solutions allowed some otherwise-restricted traffic through during peak usage of the network. While we admit that many LANs will be limited in Internet bandwidth, it seems peculiar that we were able to circumvent the solutions' blocking mechanisms with a flood of HTTP traffic. This was true only of non-proxy-based solutions.

All testing workstations and the Web server consisted of a single-processor Pentium III 500 MHz with 256 MB of RAM. We used RadView Software's WebLoad 3.51 load-generation software to emulate the 12 clients. For the network, we used Extreme Networks' Summit24 switch and an Intel Corp. 10/100 stackable hub to provide the shared network segment for protocol-analyzer-based products.

Executive Summary -- Content Monitors

The content-monitoring products we tested do a good job of investigating and reporting your network's behavior to the powers that be. And at a price that suits most budgets, a content monitor may be a worthwhile investment. Fitting somewhere between the network protocol analyzer and a full-fledged network management solution, these products monitor and report on your network's traffic. With an emphasis on Web traffic, content monitors are capable of measuring and monitoring e-mail usage, FTP, IRC and, in some cases, popular networking games such as Quake and Duke Nukem.

Earning top honors with excellent reporting and monitoring features and superior flexibility in policy creation and management is SurfControl's SuperScout. Elron Software's CommandView Internet Manager follows a close second with top-notch monitoring features and very competitive reporting and policy-creation capabilities. The other products we tested could be ideal for particular network configurations. Secure Computing's SmartFilter and Websense's Websense Enterprise, for instance, offer seamless integration into popular proxy and firewall products, including proxy servers from Microsoft Corp. and Netscape Communications Corp., as well as Check Point Software Technologies' FireWall-1. The products from N2H2 and Internet Products offer the ease of use associated with turnkey solutions while off-loading much of the content-monitoring responsibility to the services provided with each solution.

http://www.nwc.com/

Copyright © 2000 CMP Media Inc.

* * *

Network World Sept 11, 2000 pNA

Online babysitters

Finding Internet monitoring tools is no problem. Here's how to figure out which one is best for your needs.

By Tom Duffy

Colin Morrison, vice president of IS for the Kitsap Community Central Credit Union, had a problem.

Plans called for the Bremerton, Wash., credit union to install Internet-accessible computer kiosks in 10 branches for customer Web banking demonstrations. But Morrison worried where Web surfers might wander. "My biggest concern was that little Johnny would come in with mom, and while mom was in line for the teller, he'd be surfing at hooters.com," Morrison says.

Morrison's concerns may have centered on the curiosities of youngsters, but they're much like those of many IT executives. IT folks are on the hot seat, charged with stopping illicit Internet and e-mail use. Fueled by corporate fear of sexual harassment and other liability potential, the market for (and buzz surrounding) 'Net monitoring tools grows daily.

Bill Gassman, an analyst for Gartner Group in Stamford, Conn., believes that nearly half of all companies now monitor Internet use. Meanwhile, market research firm IDC in Framingham, Mass., projects the market for Internet access control products will grow from $63 million in 1999 to $260 million by 2003.

(Cont'd on next page)

Internet monitoring tools come in plenty of flavors. Some strictly provide reports on site visits without offering blocking capabilities. Others offer sophisticated policy engines that let administrators define Internet user access profiles, even by time of day. Network World recently reviewed nine of these tools (link to http://www.nwfusion.com/research/2000/0710feat.html.)

These tools are not interchangeable - choosing the wrong type can even create problems, such as breaches of confidentiality. Many Internet monitoring tool vendors provide user guidelines to help customers guard against problems. Some suggest Internet monitoring policies, for example, while others hand out case studies showing how companies have handled the complex issues surrounding tool use.

In his case, Morrison determined the right type of tool for his needs was one that let him strictly control access rights for user groups and individuals. He picked SurfControl from JSB Software in Scotts Valley, Calif. "If you try to go to a non-approved site, you're redirected to our home page," he says.

IT and beyond

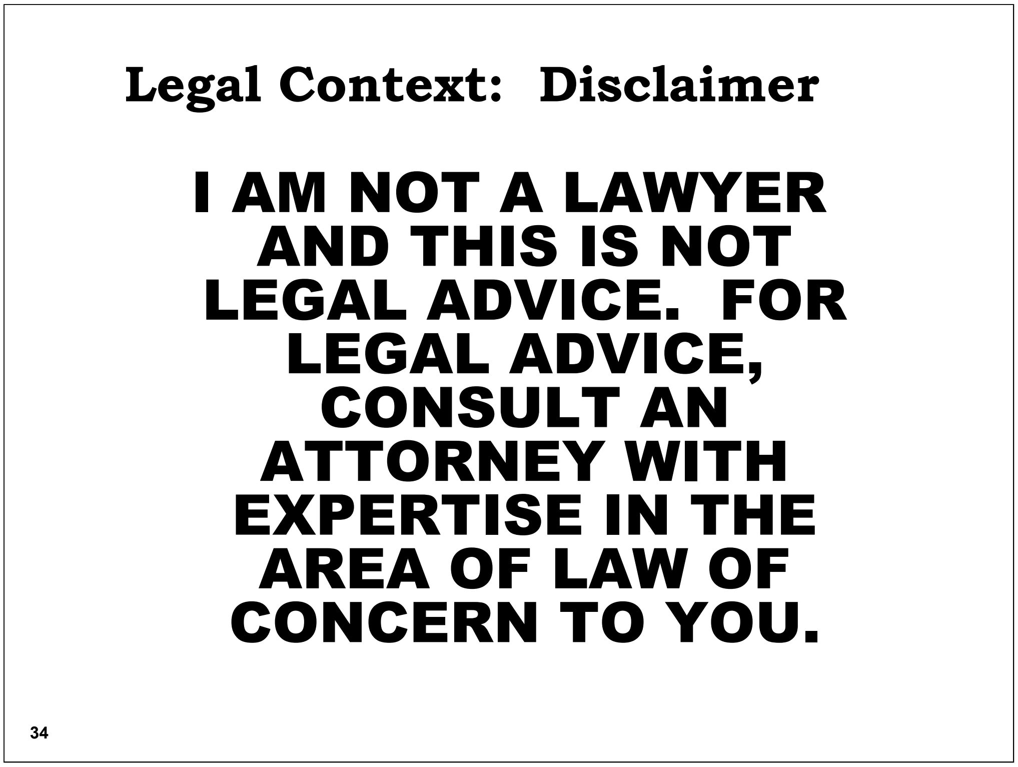
Once monitoring tools are in place, IT managers need to guard against complacency, says Mark Schreiber, a partner at Palmer & Dodge, a Boston law firm. Offensive material can easily slip onto someone's screen as an e-mail attachment, but not many companies are monitoring e-mail traffic. That task typically requires additional tools as well as a subtler approach.

What's more, you've got to team with HR. Consider it mandatory as a way to protect yourself from potential bad buzz. "IT has to run the software. But someone upstairs has to be savvy enough on HR, technology and legal fronts to make decisions about what do with this material once spotted," Schreiber says.

IT managers also must learn not to be too stringent. At Kitsap, for example, Morrison is planning to install Internet-accessible terminals in company lunchrooms so workers can use their free time for activities such as making airline reservations or buying concert tickets. Users will have unlimited Internet access from those terminals. "Since it will be public, I'm hoping peer pressure will dictate where they go," he says. But just in case, SurfControl will be on the job.

Duffy is a freelancer in Haydenville, Mass.

Copyright © 2000 Network World.

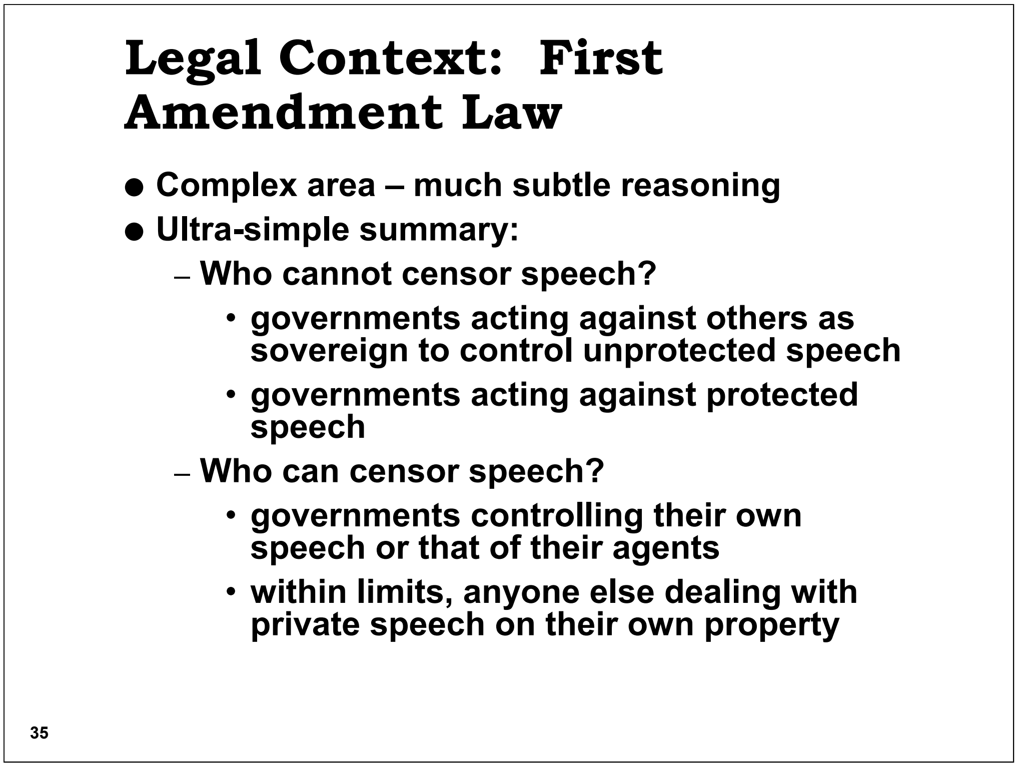


Legal Context: Disclaimer

I AM NOT A LAWYER AND THIS IS NOT LEGAL ADVICE. FOR LEGAL ADVICE, CONSULT AN ATTORNEY WITH EXPERTISE IN THE AREA OF LAW OF CONCERN TO YOU.

34

It is illegal to dispense legal advice if one is not a lawyer. The following comments are my understanding as a layman and are not to be construed as legal advice. Before making any decisions based on the information that follows, consult a trained attorney.

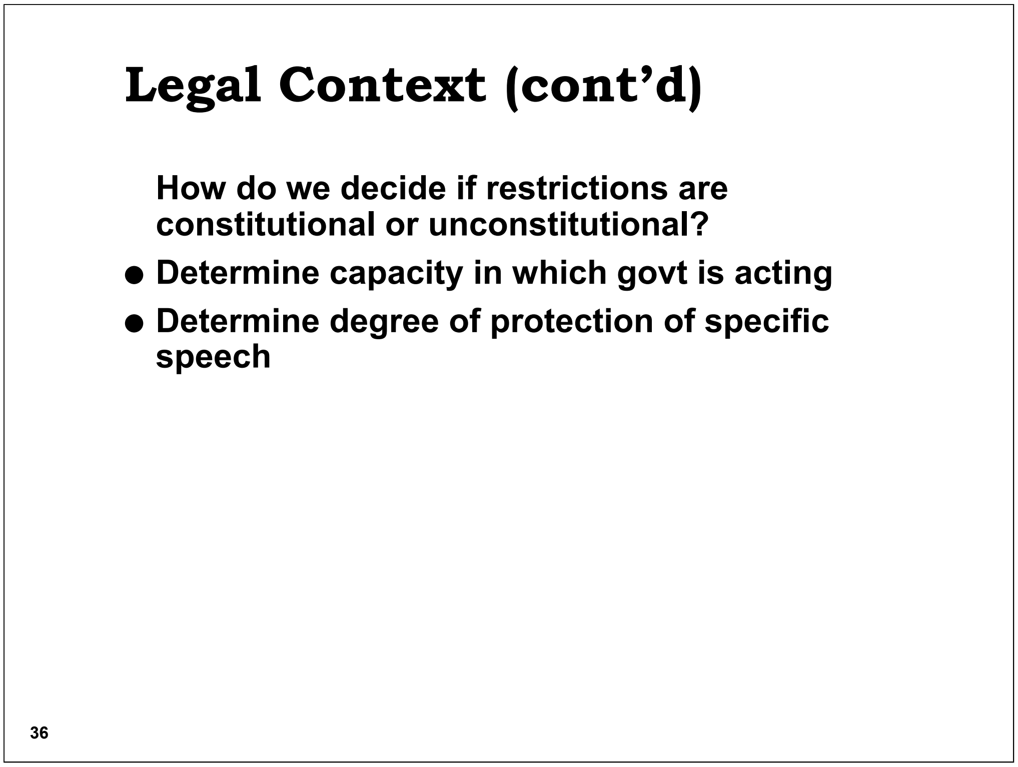


Legal Context: First Amendment Law

- Complex area – much subtle reasoning
- Ultra-simple summary:
  - Who cannot censor speech?
    - governments acting against others as sovereign to control unprotected speech
    - governments acting against protected speech
  - Who can censor speech?
    - governments controlling their own speech or that of their agents
    - within limits, anyone else dealing with private speech on their own property

35

See Lessig, L., D. Post & E. Volokh (1997). *Cyberspace Law for Non-Lawyers.* Originally published via e-mail. Available free at http://www.ssrn.com/update/lsn/cyberspace/csl_lessons.html . Provides an excellent, step-by-step introduction to laws affecting cyberspace, including 27 lessons on free speech.

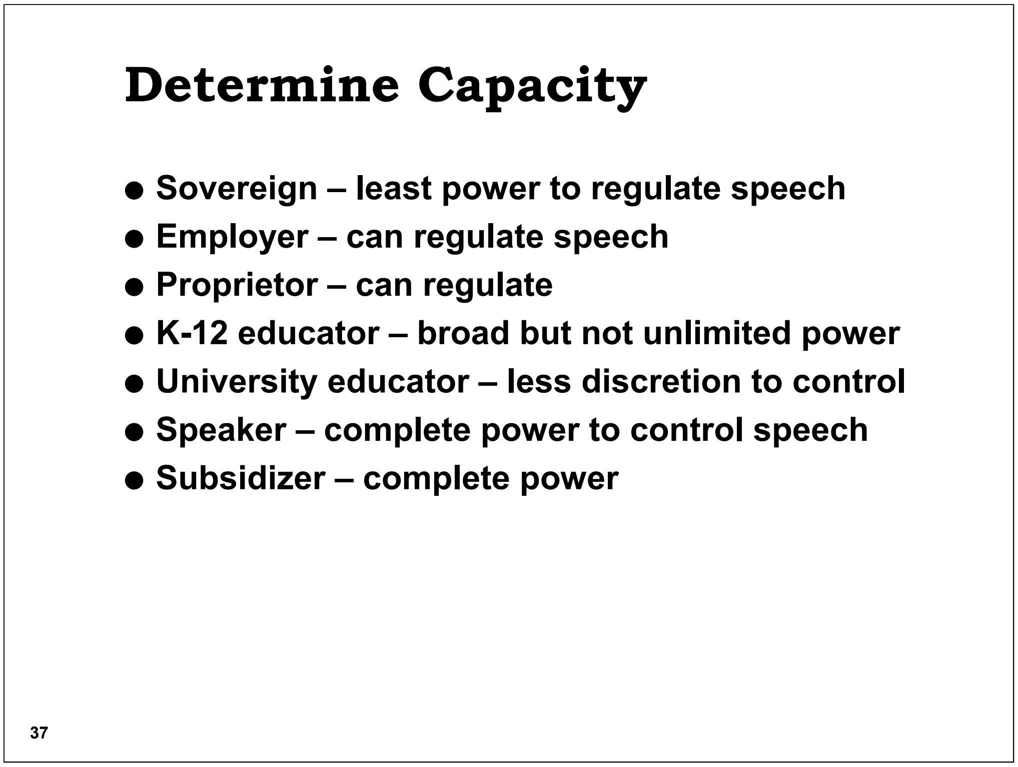


Legal Context (cont'd)

How do we decide if restrictions are constitutional or unconstitutional?

- **Determine capacity in which govt is acting**
- **Determine degree of protection of specific speech**

36



Determine Capacity

- Sovereign – least power to regulate speech
- Employer – can regulate speech
- Proprietor – can regulate
- K-12 educator – broad but not unlimited power
- University educator – less discretion to control
- Speaker – complete power to control speech
- Subsidizer – complete power

37

From *Cyberspace Law for Non-Lawyers:*

FREE SPEECH 3: IN WHAT CAPACITY IS THE GOVERNMENT ACTING?

The next step in analyzing a government-imposed speech restriction is to ask in what capacity the government is acting:

- **As SOVEREIGN:** If the government is acting in its capacity as lawmaker, controlling private people using private property, it has the least power to regulate speech. Examples: If the government bans nude pictures on all Web pages, or bans rudeness on all newsgroups, it's acting as sovereign (and, in this case, acting unconstitutionally).

- **As EMPLOYER:** If the government is constraining only what its employees say -- whether on or off the job -- it has much more discretion. (We'll explain just how much discretion it has several messages from now.) Example: If a government agency fires an employee for sending rude e-mail to a coworker, it's almost certainly acting constitutionally.

- **As PROPRIETOR**: If the government is constraining what people say on its property -- for instance, on its computers -- it also has more discretion, though how much depends on the kind of property. (Again, more on this later.) Example: If a government agency says it'll let anyone set up Web pages on its computer, but only if the pages are specifically related to issues in the upcoming election, it's almost certainly acting constitutionally.

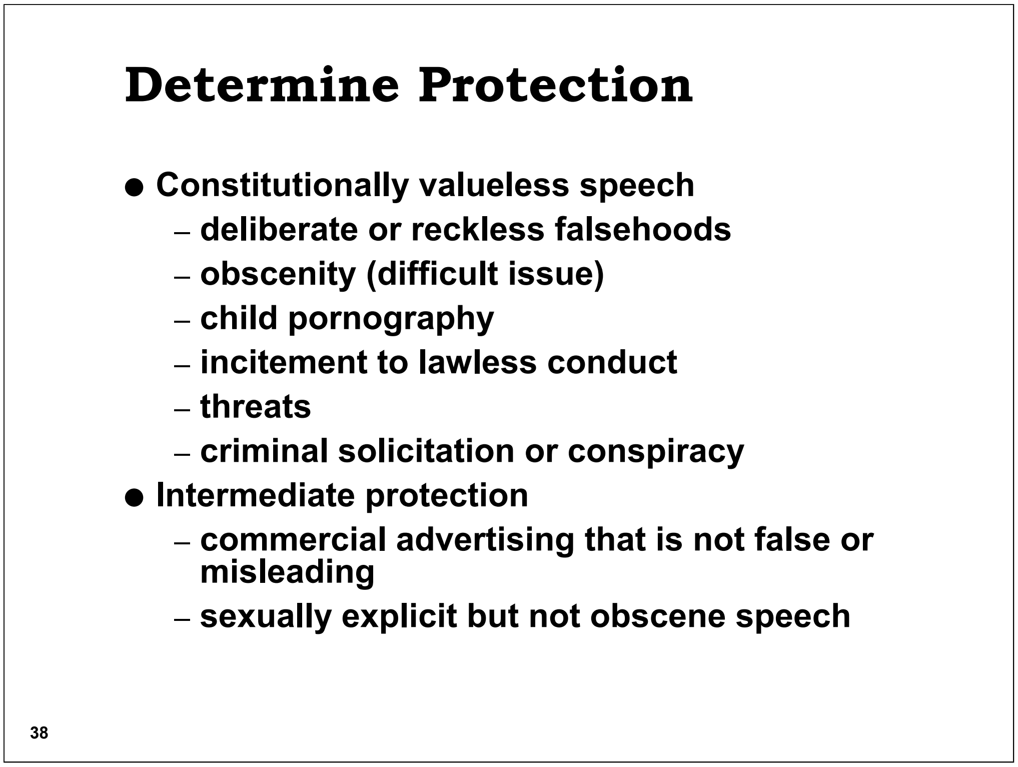
- **As K-12 EDUCATOR**: If the government is constraining what primary and secondary school students say at school, it has very broad discretion indeed, though not unlimited discretion. Example: If a public school bans all profanity in student-to-student e- mail at school, it's acting constitutionally.

- **As UNIVERSITY EDUCATOR**: As a general rule, the government doesn't have the same extra discretion with regard to college or university students. In public spaces -- quads, sidewalks, cafeterias -- at the college, and generally in dorms, the rule is the same as for the government acting as sovereign. On university computers, though, the rule is the one for the government acting as proprietor, and for university employees, the rule is the one for the government acting as employer.

- **As SUBSIDIZER**: He who pays the piper calls the tune; if the government decides to spend money on a particular kind of speech, it can demand that the money be spent on that speech and not on other speech. Example: If the government wants to spend money on a "Say No to Drugs" e-mail campaign, it can require that none of that money be spent on, say, organizing support for a "Legalize Marijuana" initiative.

- **As SPEAKER**: When the government is itself speaking, directly or indirectly, it has complete control over what goes into this speech. Example: If the Wyoming Attorney General's office sets up a Web page, it can decide what goes on that page and what that page links to. It doesn't have to offer room for opposite views, and it can make the Webmaster put up whatever messages the Attorney General wants, whether or not the Webmaster agrees with them.

Copyright © 2001 M. E. Kabay. All rights reserved.



Determine Protection

- Constitutionally valueless speech
  - deliberate or reckless falsehoods
  - obscenity (difficult issue)
  - child pornography
  - incitement to lawless conduct
  - threats
  - criminal solicitation or conspiracy
- Intermediate protection
  - commercial advertising that is not false or misleading
  - sexually explicit but not obscene speech

38

From Cyberpace Law for Non-Lawyers

FREE SPEECH 4: GOVERNMENT AS SOVEREIGN -- THREE LEVELS OF PROTECTION

Say the government is acting as sovereign. The power it has to restrict speech depends on which of the three categories the speech falls into:

- **CONSTITUTIONALLY VALUELESS SPEECH**: Some speech has (close to) no constitutional protection, because the Supreme Court has concluded that it lacks constitutional value.

This generally includes:

* False statements of fact said by people who know the statements are false (or who show reckless disregard of the possibility of falsehood).

* Obscenity (more about that later).

* Child pornography.

* Statements that are intended to, and likely to, incite more or less immediate lawless conduct.

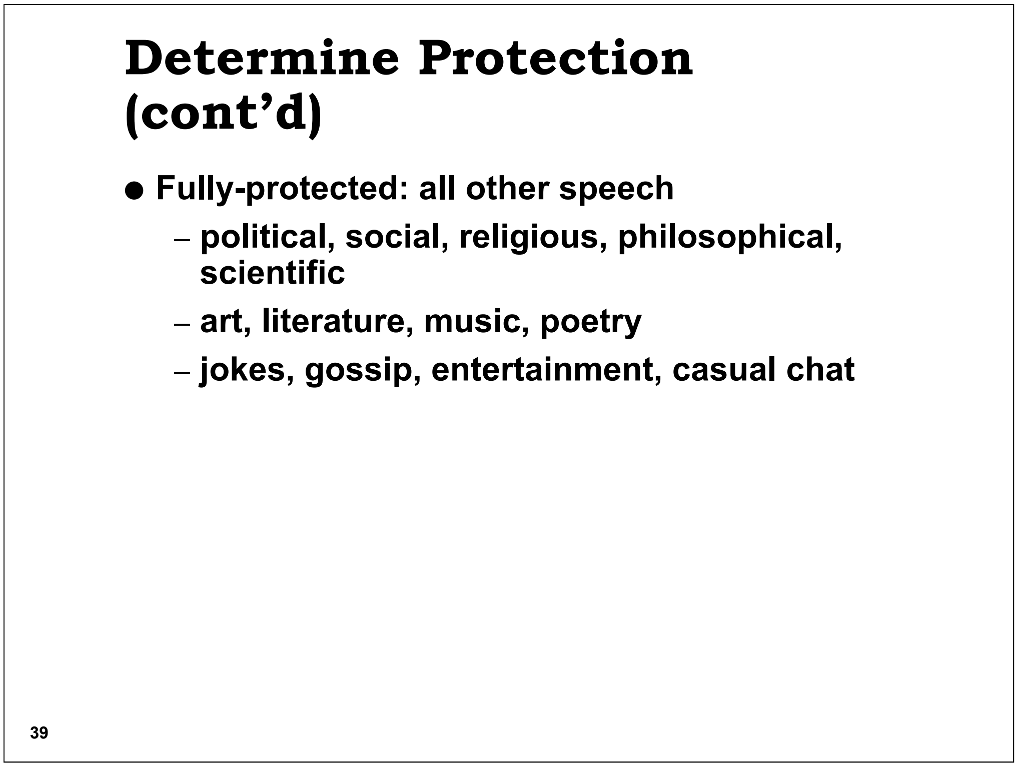
* Threats.

•Criminal solicitation or conspiracy.

- **SPEECH GIVEN INTERMEDIATE PROTECTION**: Some speech is protected to some extent, but not entirely: * Commercial advertising is unprotected if it's false (even negligently false) or misleading; it may also be unprotected in some other cases.

* Speech that is not obscene but quite sexually explicit also has some protection, but in some respects not as much protection as "fully protected"speech.

(Cont'd on next page)



Determine Protection (cont'd)

- **Fully-protected: all other speech**
  - **political, social, religious, philosophical, scientific**
  - **art, literature, music, poetry**
  - **jokes, gossip, entertainment, casual chat**

Cont'd from preceding page

- FULLY PROTECTED SPEECH: All other speech has maximum constitutional protection. This includes:

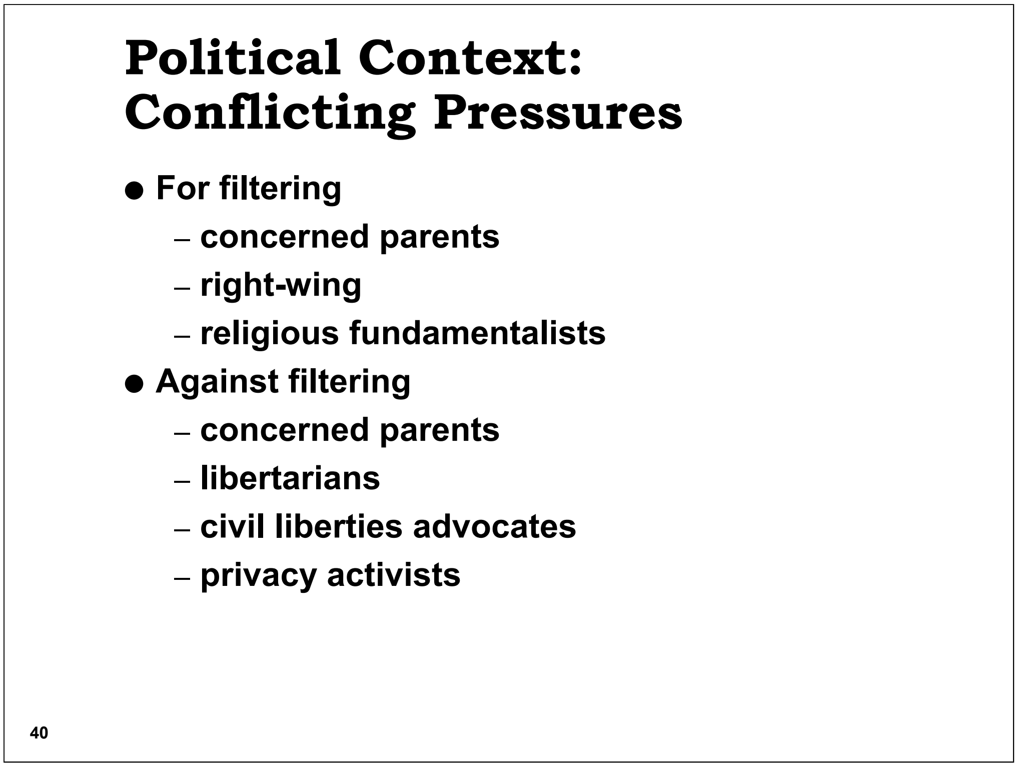
* Speech about politics, society, religion, philosophy, and science.

* Art, literature, music, poetry.

* Jokes, gossip, entertainment, and casual chit-chat.

* Pretty much anything else that doesn't fall into the valueless or intermediate categories.

Common MYTH: "Only political speech is fully protected." No; to be fully protected, speech doesn't have to be political or in any way exalted -- it just has to be outside the valueless or intermediate boxes.



Political Context: Conflicting Pressures

- For filtering
  - concerned parents
  - right-wing
  - religious fundamentalists
- Against filtering
  - concerned parents
  - libertarians
  - civil liberties advocates
  - privacy activists

Network World July 3, 2000
Senate approves Internet filtering amendment -- By Margret Johnston

Schools and libraries that receive federal funds to help pay for their Internet access would be required to add filtering software to their systems under an amendment to an appropriations bill approved by the U.S. Senate.

The Senate Tuesday voted 95-3 to require schools and libraries receiving so-called "E-rate funds" to use technology that blocks access by minors to obscenity, child pornography and "any other material that the library determines to be inappropriate for minors." The E-rate plan is part of the Telecommunications Act of 1996 and is designed to place computers with Internet access into schools and classrooms.

The amendment, submitted by Senator John McCain (R-Ariz.) comes less than a week after Congress' latest attempt to protect children from harmful material on the Internet - the Child Online Protection Act (COPA) - was rejected by an appeals court. The Third Circuit Court of Appeals in Philadelphia ruled COPA, signed into law by U.S. President Bill Clinton in 1998, unconstitutional.

The Senate also approved an amendment similar to McCain's that would require that schools and libraries either install blocking technology or adopt acceptable use policies. The amendment, put forth by Senator Rick Santorum (R-Penn.) passed 75-24.

The amendments were added to the appropriations bill for the departments of Labor, Health and Human Services and Education. The Senate is expected to vote on the full appropriations bill later this week and send it to the joint House-Senate Conference Committee, which would iron out the differences. The House already has approved the bill.

Under a third amendment added by the Senate yesterday, ISPs with 50,000 or more subscribers would be required to provide filtering software to their customers for free or at cost.

The Center for Democracy and Technology, the American Library Association, the American Civil Liberties Union and other groups opposed the McCain mandatory filtering amendment.

COPYRIGHT 2000 Network World, Inc.

From **Center for Democracy and Technology** http://www.cdt.org

Broad Opposition to Filtering Mandates Emerges - October 12, 2000

A coalition of organizations from across the political spectrum has come together to oppose federal attempts to mandate Internet filtering in libraries and schools. CDT is one of a large group of organizations--civil libertarian, public-interest, educational, corporate, and conservative--that publicly oppose filtering mandates as an inappropriate intrusion by the federal government. A bipartisan group of Senators has joined CDT in advocating against filtering mandates. Senators Patrick Leahy (D-VT), Jim Jeffords (R-VT), and Jack Reid (D-RI) have issued an important letter urging their colleagues to oppose the current draft of filtering legislation.

* * *

Letter from Sens. Leahy, Jeffords, and Reed
United States Senate
Committee on the Judiciary
Washington, DC 20510-6275

October 20, 2000

The Honorable Arlen Specter
Chairman
Subcommittee on Labor, Health and Human Services, and Education
Committee on Appropriations
Washington, D.C. 20510
The Honorable Tom Harkin
Ranking Minority Member
Subcommittee on Labor, Health and Human Services, and Education
Committee on Appropriations
Washington, D.C. 20510

Dear Chairman Specter and Senator Harkin:

We write to express our concern about and opposition to the mandatory Internet filtering language included in the conference draft of the Labor, Health, Human Services and Education Appropriations bill (H.R. 4577).

When Senator McCain brought his amendment on school and library filtering to the floor of the Senate during our debate on this bill, he worked with Senator Leahy to include the language Senator Hatch and Senator Leahy had previously proposed requiring large Internet service providers to make technological tools such as filtering software available to subscribers, either for free or at cost. As a result of his willingness to work together towards a bipartisan solution and inclusion of the Hatch-Leahy filtering amendment, we supported Senator McCain's amendment, while Senator Leahy stated in the record his objections to the mandatory filtering part of the amendment and his intent to address in conference the serious concerns we had to that part of the amendment.

Unfortunately, the Hatch-Leahy proposal, which would help families with Internet access on their home computers as well as schools and libraries, gain affordable access to filtering technology, should they choose to use it, has apparently been dropped from the final bill.

We all share the same concerns about protecting children from exposure to obscene and otherwise inappropriate material on the Internet. We have worked closely with Senators on both sides of the aisle to promote legislation to make technological tools available to and affordable for parents. We have supported private sector educational efforts such as America Links Up and GetNetWise to help educate parents and caregivers about children's online safety, and on how to find ways to protect children that respect the diverse values of American families.

The sweeping mandatory Internet filtering requirements for schools and libraries in the draft conference report for FY01 Labor-HHS-Education Appropriations bill, H.R. 4577, goes much further than anything the Senate has previously considered and will substantially harm, not help, the children of this Nation. This amendment would require schools and libraries to certify, install and enforce an Internet filtering program, under the supervision of the Federal Communications Commission (FCC) and under threat both of losing their E-rate discounts and other critical federal assistance in the future and the financial liability of having to reimburse federal funds they have already spent.

Our serious concerns with these mandatory filtering requirements are summarized below.

(Cont'd on next page)

First, the mandatory filtering provisions in the conference report turn federalism principles on their head. These provisions would put the federal government and various federal agencies in charge of what is decidedly a local matter. Specifically, these provisions require that schools and libraries obtaining E-rate discounts for telecommunications services, or other federal assistance, use blocking and filtering software that makes inaccessible material that is obscene, child pornography or harmful to minors, even if local authorities determine that other strategies are more appropriate for both students and library patrons. Schools and libraries that opt for alternative strategies and choose not to install and use filtering software forfeit not only their E-rate discounts, but also other federal assistance to fund the cost of computers or Internet connectivity.

Second, the mandatory filtering provisions would invite the Federal Communications Commission (FCC) to be the de facto national censor, collecting from schools and libraries around the country so-called "certifications" that they are implementing blocking and filtering programs on computers with Internet access and blocking material that is obscene, child pornography or harmful to minors. The FCC would be responsible for policing these schools and libraries to ensure that they are fulfilling the promises they make in the certifications, and are in fact blocking computer access to such inappropriate material. Moreover, the FCC would also be the ultimate enforcer with responsibility for determining when schools and libraries have failed to comply with the certification requirements of the law and failed "to ensure the use of its computers in accordance with a certification."

In practical terms, the FCC would be reconstituted into an updated version of the Meese Commission on Pornography, but with far greater enforcement powers and coercive effect. As part of the certification process mandated in these provisions, schools and libraries would likely seek to submit their plans for Internet filtering to the Commission for guidance on whether their Internet use policies are acceptable. This would require the FCC to make literally thousands of determinations as to what constitutes "obscene material," "child pornography" or "material harmful to minors" in order to provide comfort to schools and libraries seeking guidance. The financial risks are too great for schools and libraries to simply wait for the FCC to find their filtering and compliance plans to be insufficient. This will, in the end, defeat the local decision-making to which these provisions pay lip service.

Other federal agencies would have similar censorship-like responsibilities under the mandatory filtering provisions. For example, the Secretary of Education would be required to enforce blocking and filtering programs in schools receiving funds under Title III of the Elementary and Secondary Education Act of 1965 (ESEA), with authority to "issue a complaint to compel compliance through a cease and desist order." The National Telecommunications and Information Administration (NTIA) would be charged with "evaluating the development and effectiveness of local Internet use policies that are currently in operation..." No school or library would want to be on NTIA's list of ineffective local Internet use policies, with the risk that might pose to critical federal funding.

Third, the mandatory filtering provisions would result in broad "self-censorship" by schools and libraries and lead to a chilling of free speech to the detriment of our nation's children and library patrons. To ensure their filtering programs pass muster with the FCC or Secretary of Education or the NTIA and their continued eligibility for the E-rate and to avoid having to reimburse past financial discounts, schools and libraries may go overboard and block out material deemed by any vocal minority to be inappropriate. School boards and libraries faced with the risk of losing federal funding assistance can be expected to implement highly restrictive programs. A simpler and more practical solution would be for libraries to put the computer monitors in open areas; it is hard to imagine children who are going to download objectionable material where anyone walking by can see what they are doing.

Fourth, the mandatory filtering provisions would create a disincentive for schools and libraries from using federal funds or E-rate discounts for Internet connectivity. Specifically, the provisions expressly provide that schools and libraries may avoid the certification requirements and the concomitant risk to their federal funding, if that funding is used "only for purposes other than the provision of Internet access, Internet services, or internal connection."

Schools and libraries may be sorely tempted to forego federal funding assistance and the increased Internet connectivity these funds may pay for since the FCC certification and other monitoring requirements in these mandatory filtering provisions will be a paperwork nightmare and place significant regulatory burdens on financially strapped schools and libraries. Schools and libraries have to certify different aspects of this proposal to

(Cont'd on next page)

the FCC, the Department of Education, and Institute of Museum and Library Services. Depending on the funding source paying for the technology, a 17 year old may be allowed to use the Internet as if he were a child or an adult, requiring schools and libraries to closely track the ages of older minor students and library patrons. Several school and library groups have begun drafting a "Step by Step" guide to help their local members understand their legal obligations if these provisions become law. This guide is more than 15 pages long and requires hundreds of steps for a school or library to determine whether or not it is in compliance with the requirements. This is an enormous burden on schools and libraries.

Fifth, the mandatory filtering provisions would adversely affect the use of computers in schools and libraries by adults. The original McCain amendment did not require schools and libraries with only one computer connected to the Internet to use filtering technology, nor did it require that adults prove to librarians that they were engaged in "bona fide research or other lawful activities" in order for an adult to gain unfiltered access to constitutionally protected material on the Internet. These new requirements in the conference report for adult use of computers in schools and libraries put the administrator of the school or library in the position of screening an adult's use of the computer, with obvious implications for the privacy and confidentiality of the adult's computer use and the possible chilling effect such a "gate-keeping" function will have on such use.

Finally, the mandatory filtering provisions in the conference report create new possibilities for the collection of personally identifiable information about children's use of the Internet in schools. Schools are required to "monitor" children's use of the Internet through either technical or personal supervision means. While we support teacher supervisions of children using the Internet, a federal mandate in this area is troubling. If students have access to school e-mail accounts from home, must the school track and read that child's e-mail? If the school chooses to install technological monitoring software, what happens to the data created by that software? Who has access to it? How long is it kept, and how securely?

In sum, this sweeping federal mandate is the wrong approach to protecting children on the Internet. That is why the mandatory filtering proposal in the conference report is opposed by the American Association of School Administrators, the American Association of University Women, the American Library Association, the Association of Educational Service Agencies, the Council of Chief State School Officers, the Council of the Great City Schools, the Consortium for School Networking, the International Society for Technology in Education, the National Association of Elementary School Principals, the National Association of Independent Schools, the National Association of Secondary School Principals, the National Education Association, the National PTA, the National Rural Education Association, the National School Boards Association, People for the American Way, the Rural School and Community Trust, the Free Congress Foundation, Americans for Tax Reform, the Small Business Survival Committee, the American Family Association of Oregon, and the Software and Information Industry Association.

Indeed, the Children's Online Protection Act (COPA) Commission has today delivered recommendations to the Congress. They recommend, and we have always supported, focusing on educating families about Internet safety, educating parents about their choices if they want to use Internet filters in the home, and on enforcing existing, constitutional laws against criminal conduct involving the Internet. The Commission does not support mandatory filtering laws but urges voluntary adoption of acceptable use policies.

We urge you to address the problems with the mandatory filtering provision in the current draft of the conference report. Alternatively, we urge you to eliminate these provisions so that, with the benefit of the COPA Commission report and recommendations, we can craft a responsible, constitutional, workable and effective solution to protecting children from inappropriate online content.

Sincerely,

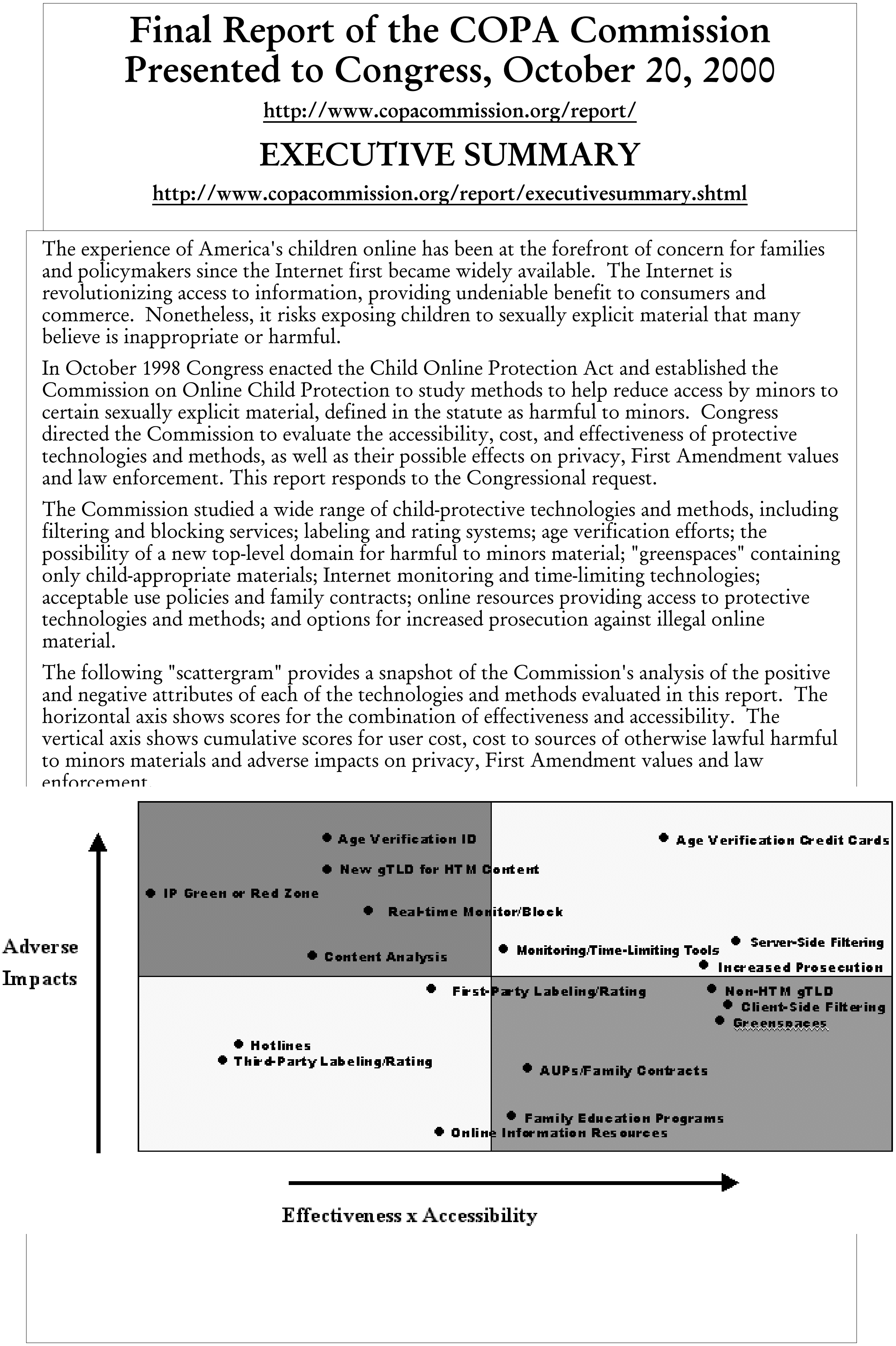
PATRICK LEAHY
United States Senator

JIM JEFFORDS
United States Senator

JACK REED
United States Senator

cc
Chairman Stevens
Senator Byrd
Senator McCain
Senator Santorum

Copyright © 2001 M. E. Kabay. All rights reserved.



Final Report of the COPA Commission Presented to Congress, October 20, 2000

http://www.copacommission.org/report/

EXECUTIVE SUMMARY

http://www.copacommission.org/report/executivesummary.shtml

The experience of America's children online has been at the forefront of concern for families and policymakers since the Internet first became widely available. The Internet is revolutionizing access to information, providing undeniable benefit to consumers and commerce. Nonetheless, it risks exposing children to sexually explicit material that many believe is inappropriate or harmful.

In October 1998 Congress enacted the Child Online Protection Act and established the Commission on Online Child Protection to study methods to help reduce access by minors to certain sexually explicit material, defined in the statute as harmful to minors. Congress directed the Commission to evaluate the accessibility, cost, and effectiveness of protective technologies and methods, as well as their possible effects on privacy, First Amendment values and law enforcement. This report responds to the Congressional request.

The Commission studied a wide range of child-protective technologies and methods, including filtering and blocking services; labeling and rating systems; age verification efforts; the possibility of a new top-level domain for harmful to minors material; "greenspaces" containing only child-appropriate materials; Internet monitoring and time-limiting technologies; acceptable use policies and family contracts; online resources providing access to protective technologies and methods; and options for increased prosecution against illegal online material.

The following "scattergram" provides a snapshot of the Commission's analysis of the positive and negative attributes of each of the technologies and methods evaluated in this report. The horizontal axis shows scores for the combination of effectiveness and accessibility. The vertical axis shows cumulative scores for user cost, cost to sources of otherwise lawful harmful to minors materials and adverse impacts on privacy, First Amendment values and law enforcement.

Technologies and methods identified in the lower right quadrant are most effective and accessible while imposing fewer costs and adverse impacts. Those identified in the upper left quadrant are relatively ineffective and create the most adverse effects.After consideration of the information gathered through hearings and comments filed by a wide range of parties, the Commission concludes that no single technology or method will effectively protect children from harmful material online. Rather, the Commission determined that a combination of public education, consumer empowerment technologies and methods, increased enforcement of existing laws, and industry action are needed to address this concern. The Commission's specific recommendations are as follows:

Public Education:

Government and the private sector should undertake a major education campaign to promote public awareness of technologies and methods available to protect children online.

Government and industry should effectively promote acceptable use policies.

Consumer Empowerment Efforts:

Resources should be allocated for the independent evaluation of child protection technologies and to provide reports to the public about the capabilities of these technologies.

Industry should take steps to improve child protection mechanisms, and make them more accessible online.

A broad, national, private sector conversation should be encouraged on the development of next-generation systems for labeling, rating, and identifying content reflecting the convergence of old and new media.

Government should encourage the use of technology in efforts to make children's experience of the Internet safe and useful.

Law Enforcement:

Government at all levels should fund, with significant new money, aggressive programs to investigate, prosecute, and report violations of federal and state obscenity laws, including efforts that emphasize the protection of children from accessing materials illegal under current state and federal obscenity law.

State and federal law enforcement should make available a list, without images, of Usenet newsgroups, IP addresses, World Wide Web sites or other Internet sources that have been found to contain child pornography or where convictions have been obtained involving obscene material.

Federal agencies, pursuant to further Congressional rulemaking authority as needed, should consider greater enforcement and possibly rulemaking to discourage deceptive or unfair practices that entice children to view obscene materials, including the practices of "mousetrapping" and deceptive meta-tagging.

Government should provide new money to address international aspects of Internet crime, including both obscenity and child pornography.

Industry Action:

The ISP industry should voluntarily undertake "best practices" to protect minors.

The online commercial adult industry should voluntarily take steps to restrict minors' ready access to adult content.

Conclusion

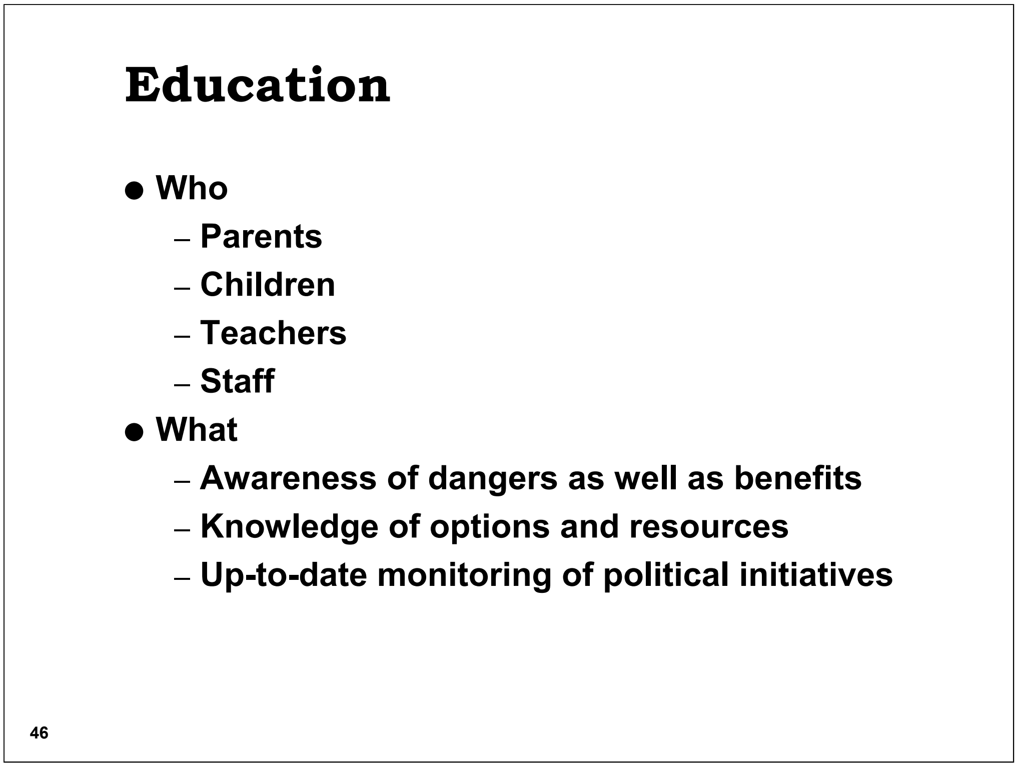
The child-protective technologies and methods evaluated by the Commission provide an important but incomplete measure of protection from harmful to minors material online. The efforts recommended in this report, if implemented by industry, consumers, and government, will result in significant improvements in protection of children online.

* * *

This is an abbreviated version of the recommendations. The full text of the Commission's recommendations can be found at pp. 39 to 46 of the Report.

webmaster@copacommission.org /

Copyright © 2000 COPA Commission



Education

- Who
  - Parents
  - Children
  - Teachers
  - Staff
- What
  - Awareness of dangers as well as benefits
  - Knowledge of options and resources
  - Up-to-date monitoring of political initiatives

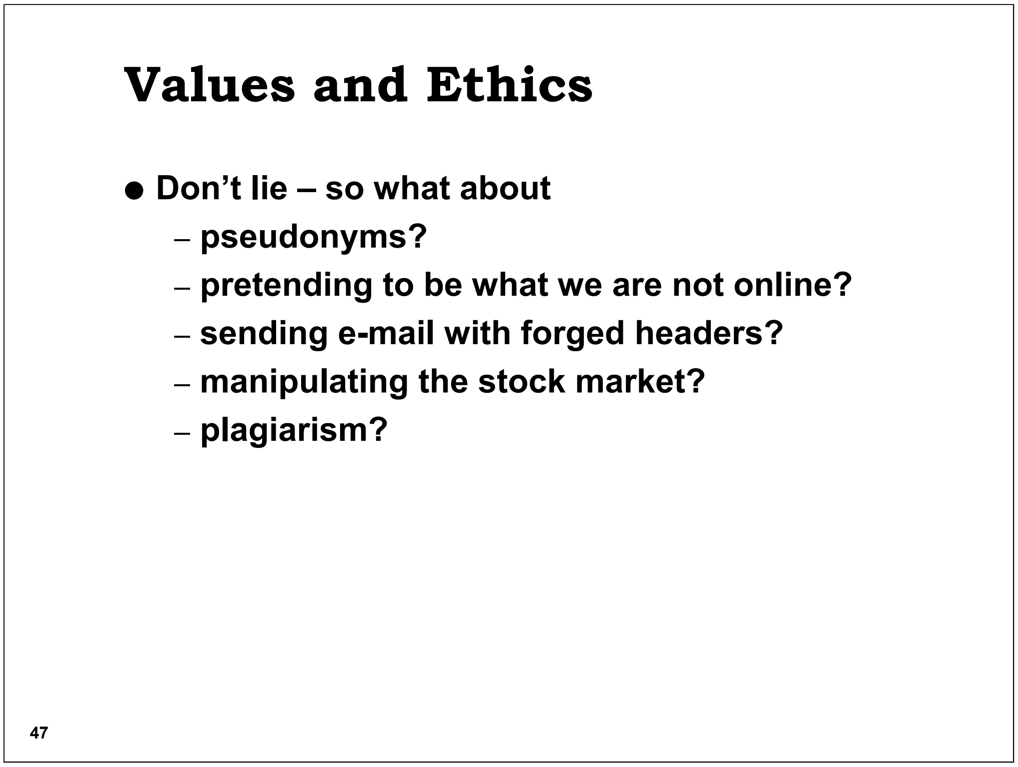
46

For further reading:

Kabay, M. E. (2000). Why Kids Shouldn't Be Criminal Hackers, v07.
http://securityportal.com/cover/coverstory20001009.html and also
http://tscorp.icsa.net/html/secsol/whitepapers/kids_criminal_hackers.pdf

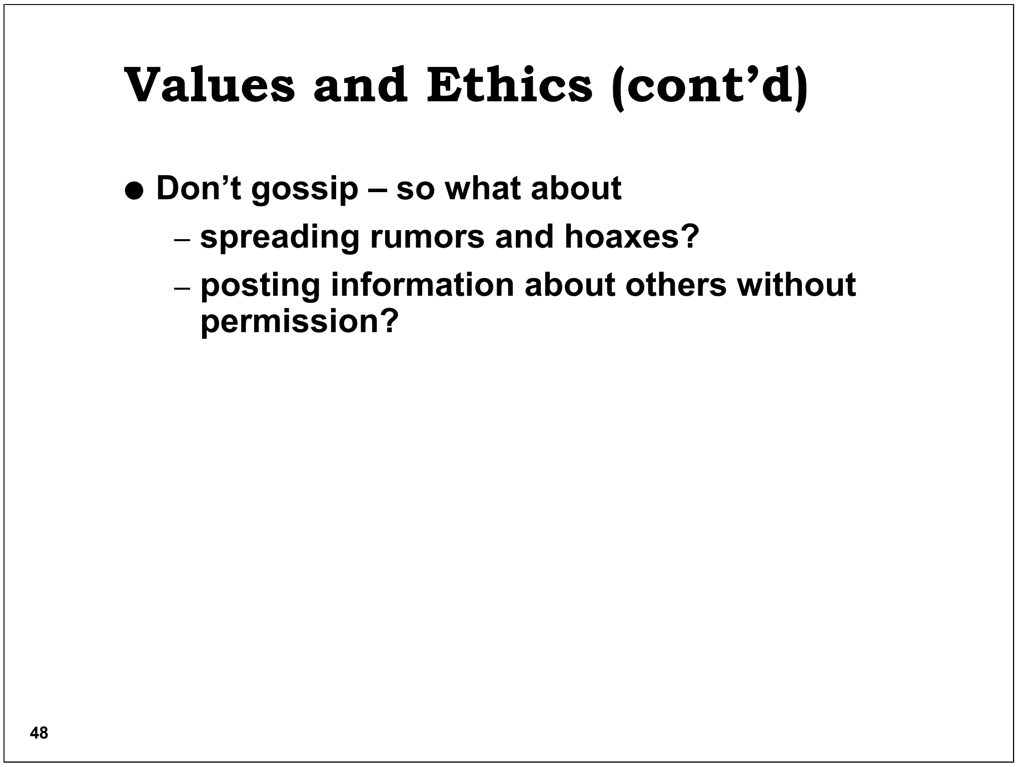
Kabay, M. E. (2000). The Napster Cantata.
http://www.securityportal.com/articles/napster20001013.html

Copyright © 2001 M. E. Kabay. All rights reserved.



Values and Ethics

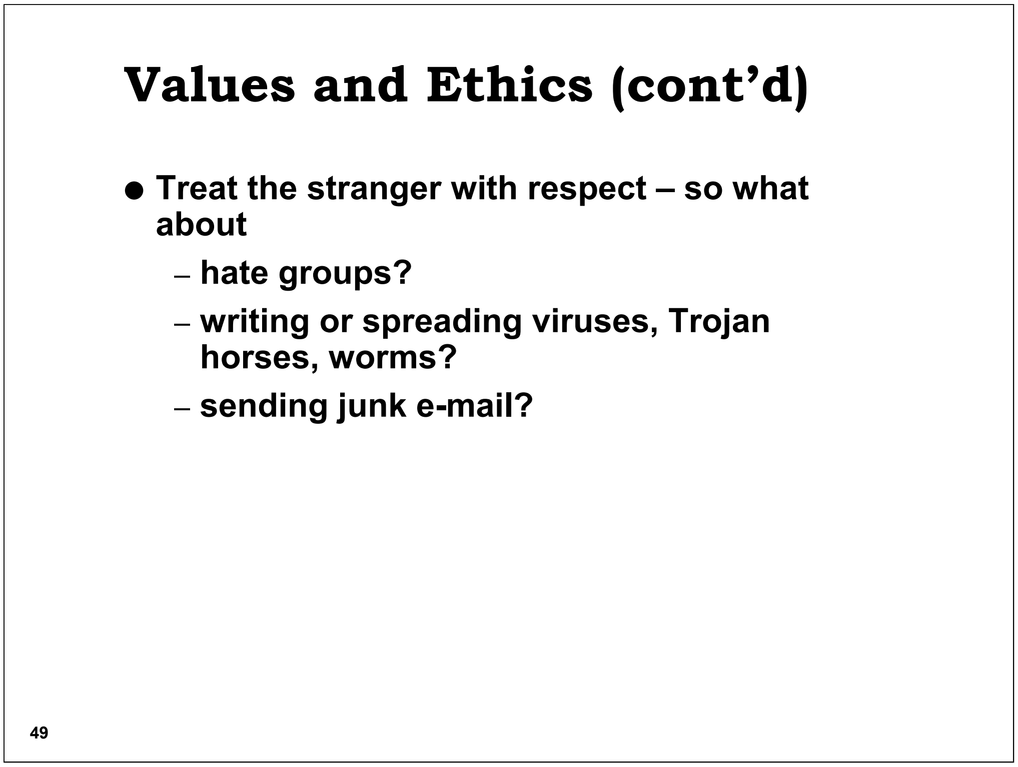
- **Don’t lie – so what about**
  - **pseudonyms?**
  - **pretending to be what we are not online?**
  - **sending e-mail with forged headers?**
  - **manipulating the stock market?**
  - **plagiarism?**



Values and Ethics (cont'd)

- **Don't gossip – so what about**
  - **spreading rumors and hoaxes?**
  - **posting information about others without permission?**

Copyright © 2001 M. E. Kabay. *All rights reserved.*

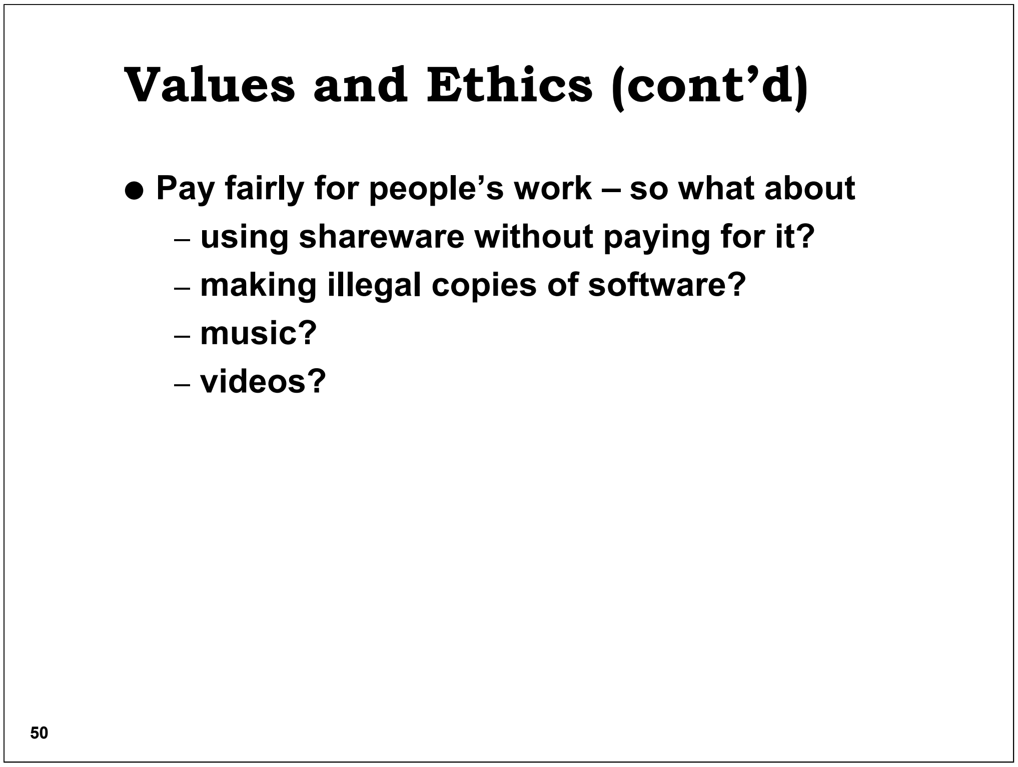


Values and Ethics (cont'd)

- **Treat the stranger with respect – so what about**
  - **hate groups?**
  - **writing or spreading viruses, Trojan horses, worms?**
  - **sending junk e-mail?**

Copyright © 2001 M. E. Kabay.

All rights reserved.

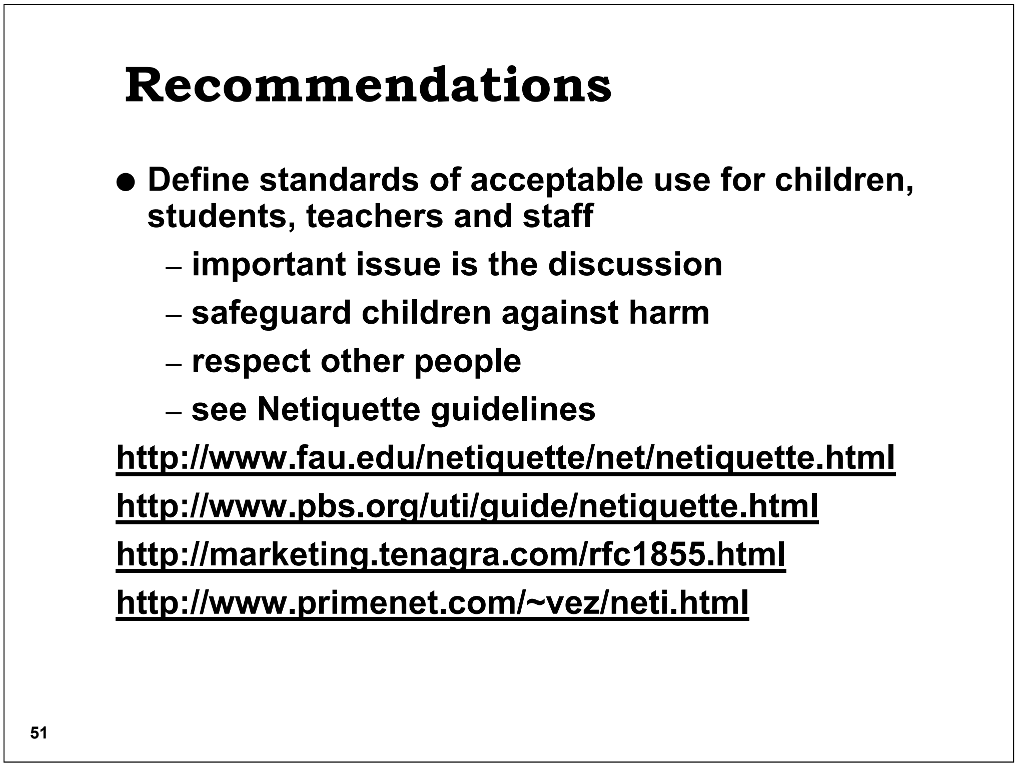


Values and Ethics (cont’d)

- **Pay fairly for people’s work – so what about**
  - **using shareware without paying for it?**
  - **making illegal copies of software?**
  - **music?**
  - **videos?**

Copyright © 2001 M. E. Kabay.

All rights reserved.



Recommendations

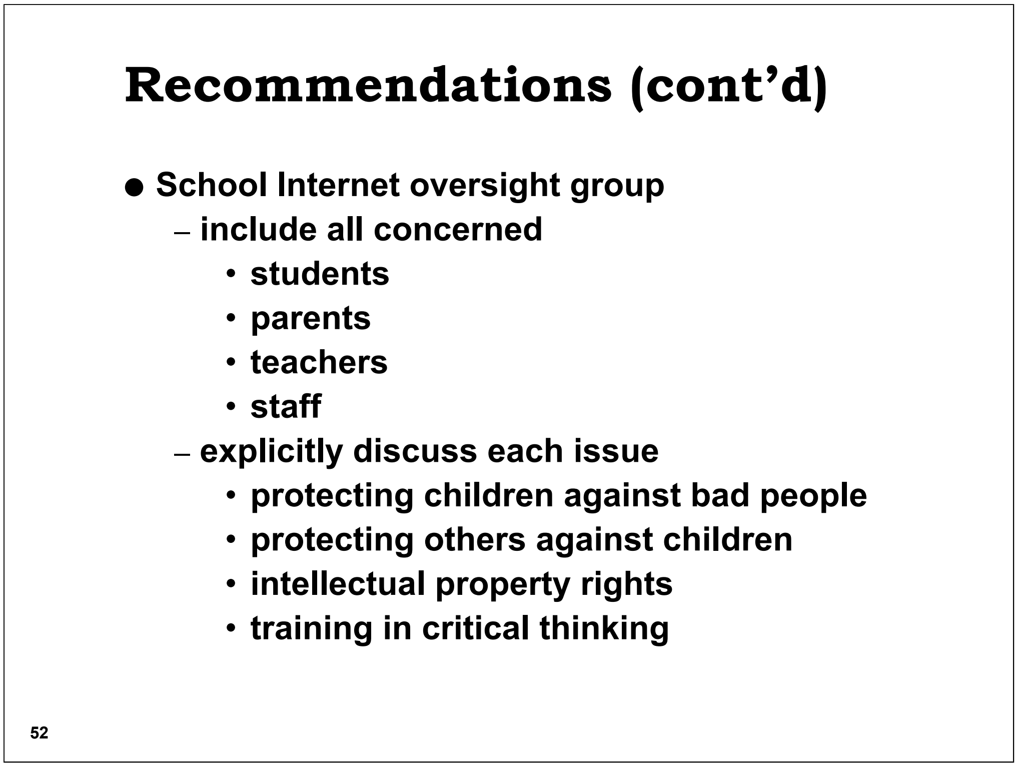
- Define standards of acceptable use for children, students, teachers and staff
  - important issue is the discussion
  - safeguard children against harm
  - respect other people
  - see Netiquette guidelines

http://www.fau.edu/netiquette/net/netiquette.html

http://www.pbs.org/uti/guide/netiquette.html

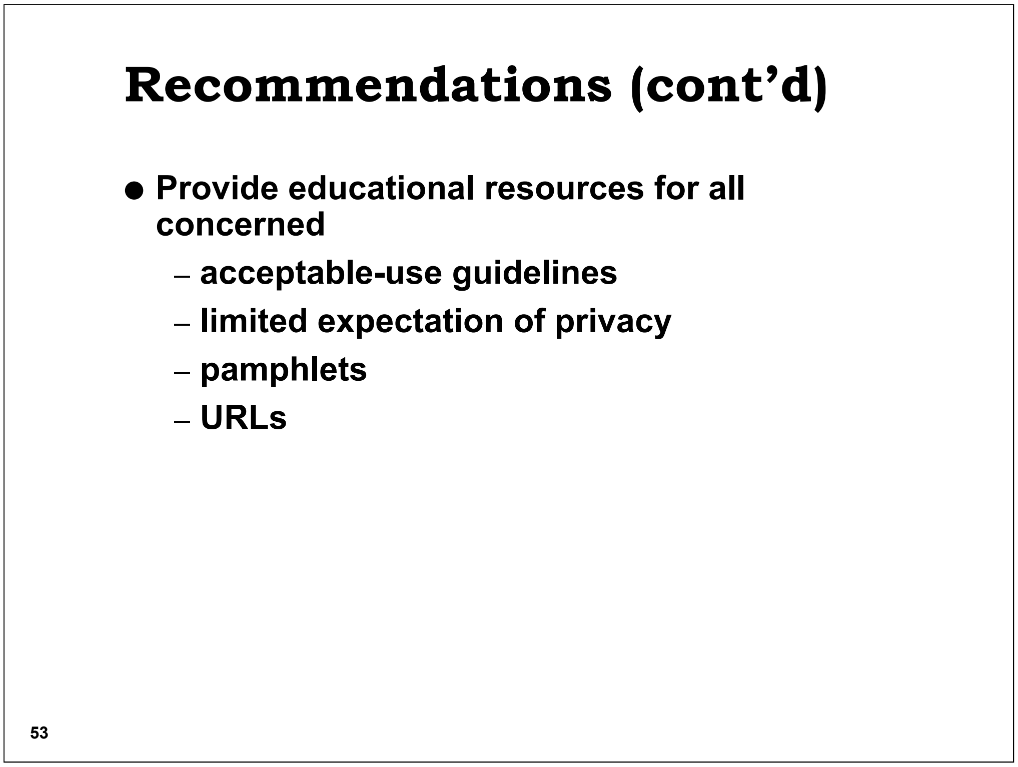
http://marketing.tenagra.com/rfc1855.html

http://www.primenet.com/~vez/neti.html



Recommendations (cont'd)

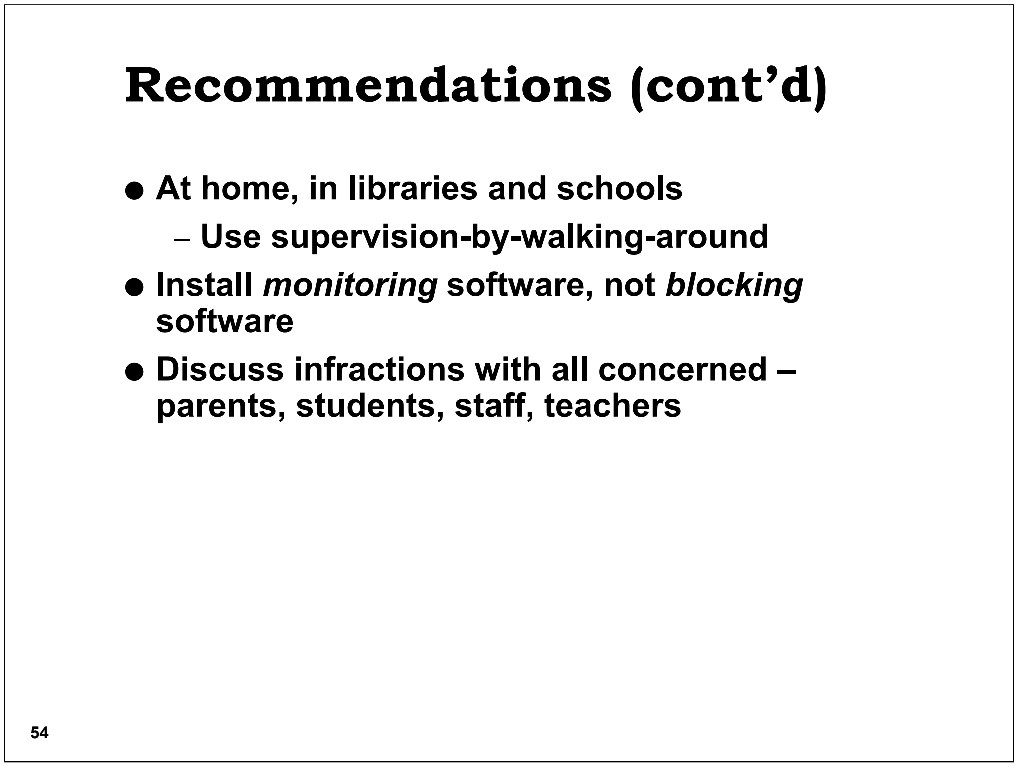
- **School Internet oversight group**
  - **include all concerned**
    - **students**
    - **parents**
    - **teachers**
    - **staff**
  - **explicitly discuss each issue**
    - **protecting children against bad people**
    - **protecting others against children**
    - **intellectual property rights**
    - **training in critical thinking**



Recommendations (cont'd)

- **Provide educational resources for all concerned**
  - **acceptable-use guidelines**
  - **limited expectation of privacy**
  - **pamphlets**
  - **URLs**

53



Recommendations (cont'd)

- At home, in libraries and schools
  - Use supervision-by-walking-around
- Install *monitoring* software, not *blocking* software
- Discuss infractions with all concerned – parents, students, staff, teachers

DISCUSSION

55